116 سلسلة محاضرات الإمارات

مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية

الدكتور ناصر بن محمد البقمي



مركز الإمارات للدراسات والبحوث الاستراتيجية

بسم الله الرحمن الرحيم

تأسس مركز الإمارات للدراسات والبحوث الاستراتيجية في 14 آذار/ مارس 1994، كمؤسسة مستقلة تهتم بالبحوث والدراسات العلمية للقضايا السياسية والاقتصادية والاجتماعية، المتعلقة بدولة الإمارات العربية المتحدة ومنطقة الخليج العربي على وجه التحديد، والعالم العربي والقضايا الدولية المعاصرة عموماً.

من هذا المنطلق يقوم المركز بإصدار «**سلسلة محاضرات الإمارات**» التي تتناول المحاضرات، والندوات، وورش العمل المتخصصة التي يعقدها المركز ضمن سلسلة الفعاليات العلمية التي ينظمها على مدار العام، ويدعو إليها كبار الباحثين والأكاديميين والخبراء؛ بهدف الاستفادة من خبراتهم، والاطلاع على تحليلاتهم الموضوعية المتضمنة دراسة قضايا الساعة ومعالجتها. وتهدف هذه السلسلة إلى تعميم الفائدة، وإثراء الحوار البنَّاء والبحث الجاد، والارتقاء بالقارئ المهتم أينما كان.

سلسلة محاضرات الإمارات

- 116 -

مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية

الدكتور ناصر بن محمد البقمي



تصدر عن

مركز الإمارات للدراسات والبحوث الاستراتيجية

محتوى المحاضرة لا يعبِّر بالضرورة عن وجهة نظر المركز

ألقيت هذه المحاضرة يوم الثلاثاء الموافق 3 كانون الثاني/ يناير 2007

الطبعة الأولى 2008

ISSN 1682-122X

ISBN 978-9948-00-949-8

توجه جميع المراسلات إلى رئيسة التحرير على العنوان التالي:

سلسلة محاضرات الإمارات ـ مركز الإمارات للدراسات والبحوث الاستراتيجية

ص. ب: 4567

أبوظبي ـ دولة الإمارات العربية المتحدة

هاتف: 4044541-9712+

فاكس: 4044542-9712+

E-mail: pubdis@ecssr.ae

Website: http://www.ecssr.ae

مقدمة

تعـد الجريمـة مـن إفـرازات الحيـاة الاجتماعيـة، كـما تعـد مظهـراً مـن مظاهرها، ونتيجة من نتائج السلوك الإنساني في علاقاتـه المـستمرة المتطـورة على مر التاريخ.

وتتطور الجريمة بتطور الحياة الإنسانية؛ وهذا ما يجعلها تحظى بالدراسة والبحث والاهتمام المستمر، وجسَّد هذا الاهتمام ظهور الأفكار الفلسفية التي تعنى بدراسة الظاهرة وبحثها من جانبين:

الجانب الأول: اجتماعي لأن الجريمة ظـاهرة مـن الظـواهر الاجتماعيـة المسلم بها، ويعد ارتكابهـا مخـلاً بالنظـام الاجتماعـي؛ وهـذا يقتـضي تحليلهـا ومعرفة أبعادها المختلفة، وصولاً إلى مواجهتها بكل الوسائل التي قد تـؤدي إلى الحد من ارتكابها.

والجانب الآخر: قانوني يعتمد على سياسة التجريم والعقاب، أولاً عـن طريق تحديد المصالح المحمية والأفعال التـي يمكـن أن تهـددها، وثانيـاً عـبر تجريمها، وتحديد العقوبة المناسبة لها. ويتم التعامـل والجريمـة بعـد وقوعهـا وفقاً لهذه السياسة، بطريقة متشابهة في أغلب الجرائم التقليديـة التـي تُوضَّـح فيها أركان الجريمة بصورة تساعد على إثباتها؛ ومن ثم معاقبة مرتكبها.

ونتيجة التطور العلمي الذي شهده العصر الحـديث، طُـوِّرت الجريمـة وظهرت نوعية من المجرمين الذين انتقلـوا بالجريمـة مـن صـفتها التقليديـة وأبعادها المحدودة إلى آفاق جديدة تعتمد على التقنية الحديثة، وتستخدمها في تنفيذ الفعل المجرم بأساليب مبتكرة وطرائق لم تكن معروفة في السابق.

وساعد على بروز هذه الجرائم ظهور تقنيات الاتصال ووسائل الحاسب الآلي، التي كوّنت من خلال اعتماد كل منهما على الآخر نظاماً جديداً هو النظام المعلوماتي الذي أصبح يستخدم في المجالات كافة؛ ليدخل في عمل الهيئات الحكومية التي تعتمد عليه بدرجة كبيرة، وبخاصة في الزمن الحالي، كما أن الاستخدام الفردي لهذا النظام أصبح جزءاً من الحياة اليومية للأفراد.

ومع أهمية التعامل بالأساليب التقنية الحديثة؛ مثل الحاسب الآلي، والإنترنت، والخدمة العظيمة التي يؤديانها، ووجود عنصرَي الخير والشر في تلك الأنشطة، ظهر الكثير من الأساليب الإجرامية المستحدثة التي تهدد مصالح الأفراد والمجتمع. وهذا فرض أهمية الحماية القانونية لمواجهة الأفعال الإجرامية المرتكبة بوساطة النظام المعلوماتي.

من هنا أصبحت حماية النظم المعلوماتية والمواقع والشبكات من أولويات الشركات الصانعة، وبالمقابل كثّف مجرمو المعلوماتية مساعيهم لزيادة نشاطهم وعملياتهم، من خلال الشبكة العالمية التي تمكنهم من الدخول إلى أصعب المواقع وأكثرها حماية، برغم جهود الحماية التقنية المبذولة لمنع جرائمهم.

ومما يزيد انتشار هذه الجرائم تطور الوسائل المعلوماتية الحديثة التي تعاظمت فرص انتشارها. وقد لفت هذا أنظار الدول والهيئات العالمية إلى إدراك خطورة تلك الجرائم، ومدى سهولة ارتكابها، وتأثيرها المباشر في جميع المجالات، بما في ذلك تهديدها للأمن بمستوياته كافة؛ وهذا ما جعل مكافحتها من أولويات المجتمع الدولي والحكومات.

ولعل أبرز العوائق القانونية التي واجهت القـانونيين المهتمـين بدراسـة الجرائم المعلوماتية، مدى إمكانية تطبيق القوانين التقليدية على هـذه الجـرائم وتكييف الأفعال المكونة لها؛ لتدخل في نطاق النصوص التي تعـالج الجـرائم التقليدية؛ وهذا ما أوجد عدداً مـن الاتجاهـات القانونيـة التـي تنـادي بـسن قوانين خاصة لمواجهة هذه الجرائم.

الفصل الأول

ماهية الجرائم المعلوماتية وأنواعها

1. تعريف المعلوماتية

"المعلوماتية" أو "علـم المعلومـات" Informatics Or Information Science: العلـم الـذي يهـتم بالموضـوعات والمعـارف المتـصلة بأصـل المعلومات، وتجميعها وتنظيمها، واختزانها واسترجاعها، وتفسيرها، وبثهـا وتحويلها واستخدامها، كما يتضمن البحث عـن تمثيـل المعلومـات في الـنظم الطبيعية والصناعية والإدارية، واستخدام الرموز و"الأكواد" Codes في نقل الرسالة والتعبير عنها بكفاءة، فضلاً عن الاهـتمام بدراسـة أسـاليب معالجـة المعلومات؛ كالنظم المعلوماتية ونظم البرمجة؛ وبعبارة مختصرة فإن المعلوماتيـة هـي: المعالجـة الآليـة للمعلومـات. أمـا تقنيـة المعلومـات فتعنـي: التـزاوج والالتحام بين تقنيات النظم المعلوماتية والاتـصالات، والاسـتعمال المتزايـد للإلكترونيات في جميع المجالات.[1]

وأول من استعمل هذا المصطلح هو ميخايوف مـدير المعهـد الاتحـادي للمعلومـات العلميـة والتقنيـة (VINTTI) بالاتحـاد الـسوفيتي، ثـم توسـع استخدامه على مستوى جغرافي واسع، وبمفاهيم متباينة.[2]

2. تعريف الجرائم المعلوماتية (Cyber crimes)

كثرت تعريفات الجرائم المعلوماتية بتعدد النظم والقوانين. ومن أهم التعريفات: تعريف منظمة التعاون الاقتصادي والتنمية (OECD) التي عرفتها بأنها: كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، ويكون ناتجاً بطريقة مباشرة أو غير مباشرة من تدخل التقنية المعلوماتية.[3]

كما جاء في مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عُقد في فيينا عام 2000، تعريف لجرائم الحاسب الآلي نصَّ في جزء منه أنه: يقصد بالجريمة المعلوماتية أي جريمة يمكن ارتكابها بوساطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب، وهذه الجريمة تشمل - من الناحية المبدئية- جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.[4]

ومن التعريفات التي تم التوسع فيها تعريف الخبير الأمريكي باركر الذي حدد مفهوماً واسعاً للجريمة المعلوماتية؛ كي يحيط بكل أشكال التعسف في مجال استخدام نظم المعلومات، فهي من وجهة نظره: كل فعل إجرامي متعمد، أياً كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل.[5]

3. حجم الجرائم المعلوماتية

حظيت الجرائم المعلوماتية بالكثير من الدراسات التي أجريت بشأنها، إلا أن المعلومات والبيانات التي انتهت إليها هذه الدراسات تنقصها الدقة في

كثير من الأحيان، كما لم تنجح في التعبير بدقة عن الصورة الحقيقية لحجم الجريمة المعلوماتية، فمعظم الحالات التي أشار إليها كثير من هذه الدراسات قد حُصِر في نطاق مكاني واحد وهو الولايات المتحدة الأمريكية، وهو ما لا يعطي مؤشراً واضحاً لحجم هذه الجريمة. كما أن كثيراً من هذه الدراسات قد استقى تلك الحالات من مصادر ربما لا تكون موثوقاً بها دوماً، وبخاصة تلك التي يتم نشرها في الصحف والمجلات.[6]

وقد أظهر التحليل الشامل للشكاوى التي قدمت إلى مركز احتيال الإنترنت الأمريكي (IFFC)، أن عدد الشكاوى التي تلقاها المركز منذ أن بدأ أعماله في أيار/ مايو 2000 حتى تشرين الأول/ أكتوبر من العام نفسه؛ أي خلال ستة أشهر فقط، قد بلغت 6087 شكوى، من ضمنها 5273 حالة تتعلق باختراق الحاسوب عبر الإنترنت، و814 حالة تتعلق بوسائل الدخول والاقتحام الأخرى؛ كالدخول عبر الهاتف، أو الدخول المباشر إلى النظام بشكل مادي. وهي لا تمثل الأرقام الحقيقية لعدد الاحتيالات الفعلية، كما أنها تتعلق فقط بجريمة الاحتيال عبر الإنترنت، التي هي أحد أنماط أخرى كثيرة لجرائم الحاسوب والإنترنت. وقد بلغت الخسائر المتصلة بهذه الشكاوى ما يقارب 4.6 ملايين دولار، وهو رقم يقارب 33٪ من حجم الخسائر الناشئة عن كل جرائم الاحتيال التقليدية المرتكبة في الفترة نفسها، كما أن نسبة 22٪ من هذه الخسائر نجمت عن شراء منتجات عبر الإنترنت، من دون أن يتم تسليم البضاعة فعلياً للمشترين، أما نسبة 5٪ منها فكانت من خلال الاحتيال ببطاقات الائتمان.[7]

وفي المملكة المتحدة أظهرت دراسة مسحية أجرتها لجنة التدقيق في إنجلترا؛ حول قضايا الاحتيال المعلوماتي وإساءة استعمال الحاسب، وشملت

6 آلاف من المؤسسات التجارية وشركات القطاع الخاص، أن ما يقرب من نصف حالات الاحتيال التي تمت ضد هذه المؤسسات والشركات قد اكتشفت مصادفة، وكبدتها خسائر قدرت بنحو مليونين ونصف مليون من الجنيهات الإسترلينية.[8]

وقد نشرت المجموعة الاقتصادية الأوربية تقريراً بعنوان: The Vulnerability of the Information Conscious Society: European Situation، اتضح فيه أن خسائر الجرائم المرتكبة عبر النظام المعلوماتي (الغش والاحتيال والسرقة والتخريب) تبلغ 6450 مليون إيكو (E.C.U)،[9] وأن معدل الخسارة الذي سببته كل جريمة يبلغ 963 ألف إيكو. كما ورد أن 15 حالة اختلاس سببت خسارة تفوق 150 ألف إيكو لكل حالة من بينها حالتان كُبِّد فيهما مصرفان كبيران خسارة تفوق 10 ملايين إيكو لكل منهما، وفي ثمانية اختلاسات صغيرة بلغ معدل الخسائر أكثر من 40 ألف إيكو. وفي أستراليا تبين أن الخسائر التي تعرضت لها في المسح القومي الذي أجراه مكتب أبحاث إساءة استخدام النظام المعلوماتي بمعهد كولفيلد Caulfield ما بين عامي 1975 و1982 هي خسائر إساءة استخدام النظام، وقدرت تلك الخسائر بـ 900 ألف دولار، وأن معدل الخسارة لكل حالة يقدر بحوالي 32 ألف دولار. وفي الإحصاء الذي أصدره نفس المكتب عام 1985 ارتفع معدل الخسارة بالنسبة إلى الحالة الواحدة إلى 77565 دولاراً.[10]

وتعد القرصنة الفكرية[11] في مجال المعلوماتية من الجرائم التي تتسبب في خسائر فادحة للأفراد والشركات والمؤسسات التجارية، وتشير بعض أرقام القرصنة في العالم إلى الحقائق الآتية:[12]

1. تصل نسبة القرصنة في فرنسا إلى 66٪ من حجم المبيعات، وفي بريطانيا وألمانيا 49٪، وفي أمريكا 35٪.

2. زيادة نسبة القرصنة في دول شرق آسيا ودول الشرق الأوسط لتصل إلى 90٪.

3. قدرت الخسائر الناتجة من القرصنة في 11 دولة في الشرق الأوسط وشمال أفريقيا بمبلغ 666 مليون دولار عام 1994.

4. بلغ حجم الخسائر في مجال المبيعات في مصر 84.1 مليون دولار؛ أي بنسبة 93٪، وفي المملكة العربية السعودية 82.3 مليون دولار؛ أي بنسبة 90٪، وفي دولة الإمارات العربية المتحدة 54.4 مليون دولار؛ أي بنسبة 99٪، وفي دولة الكويت 25.4 مليون دولار؛ أي بنسبة 98٪.

ومن المتوقع أن يزداد حجم الجرائم المعلوماتية بشكل مستمر للأسباب الآتية:

1. الاعتماد المتزايد على وسائل التقنية الحديثة وانتشار استخدام النظم المعلوماتية على جميع المستويات.

2. إمكانية تملك أجهزة التقنية الحديثة؛ لتدني أسعارها نتيجة المنافسة بين الشركات المنتجة؛ وهذا يتيح دخول أكبر عدد ممكن للنظام المعلوماتي.

3. التوسع المستمر في تقديم خدمات الشبكة المعلوماتية.

4. الاعتماد على وسائل التقنية الحديثة في التجارة الإلكترونية، والبريد الإلكتروني، والتوقيع الرقمي، وهي تعد من المجالات الخصبة لارتكاب الجرائم المعلوماتية.

وممـا يزيـد صـعوبة تحديـد حجـم الجـرائم المعلوماتيـة عـدم وجـود الإحصاءات الصحيحة، وإحجام الكثير مـن الأشـخاص والـشركات عـن التبليغ عن تلك الجرائم؛ لأسباب شخصية وعملية.

4. دوافع الجرائم المعلوماتية

أ. السعي لتحقيق الربح

يأتي السعي لتحقيق الربح في المرتبـة الأولى مـن سـلم دوافـع ارتكـاب جرائم المعلوماتية. ففي دراسة أشار إليها الأستاذ بـاركر نجـد أن نـسبة 43٪ من حالات الغش المعلن عنها قد بوشرت من أجل الحصول على المال.[13]

ب. إثبات الذات

غالباً ما يكون الدافع لدى مرتكبـي الجـرائم المعلوماتيـة هـو الرغبـة في إثبات الذات، وتحقيق انتصار على تقنية النظم المعلوماتية، من دون أن يكـون لديهم نيات آثمة.[14]

ج. التهديد والانتقام

يمكن أن يكون الدافع لارتكاب الجريمـة تعـرُّض الـشخص للتهديـد والضغط مـن الآخـرين، في مجـالات الأعـمال التجاريـة والأخـرى الخاصـة بالتجسس والمنافسة، أو سعي بعض الموظفين إلى الانتقام من المنشآت.[15] وقد يكون الهدف تهديد الشخص وابتزازه لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعين.[16]

د. الدوافع السياسية

تعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم، كما أن الأفراد قد يتمكنون من اختراق الأجهزة الأمنية الحكومية. كذلك أصبحت شبكة الإنترنت مجالاً خصباً لنشر أفكار العديد من الأفراد والمجموعات، ووسيلة للترويج لأخبار وأمور أخرى قد تحمل في ثناياها مساساً بأمن الدولة، أو بنظام الحكم، أو قدحاً في رموز دولية أو سياسية والإساءة لها بالذم والتشهير.[17]

هـ. الدوافع الإرهابية

امتدت الجريمة الإلكترونية لتشمل صور الجريمة المنظمة؛ حيث ظهر الإرهاب الإلكتروني على الشبكة، وأخذت الجماعات الإرهابية مواقع لها على الإنترنت، تمارس أعمالها من خلالها؛ كالتحريض على القتل، بالإضافة إلى تعليم صنع المتفجرات والقنابل، علاوة على نشر أفكارها الإرهابية، وأصبحت تقوم بشن عملياتها الإرهابية عبر الإنترنت من خلال التلاعب بنظم وبيانات نظم خاصة.[18]

5. خصائص الجرائم المعلوماتية

من خصائص الجريمة المعلوماتية سرعة التنفيذ، بحيث يمكن تنفيذها خلال جزء من الثانية، وبصورة خفية لا يلحظها المجني عليه، كما أنها تتم في بيئة خاصة هي بيئة المعالجة الآلية للبيانات، وتتميز بخطورتها المتناهية على الأفراد والحكومات والشركات؛ وهذا يهدد الأمن السياسي والأمن

الاقتصادي للدول. يضاف إلى ذلك صعوبة اكتشافها ومتابعتها وتطبيق الإجراءات الجنائية عليها، من حيث جمع الأدلة والمعاينة والتفتيش والتحقيق فيها، وإمكانية تدمير الأدلة الناجمة عنها. كما أنها تحتاج إلى خبرة فنية خاصة، هذا فضلاً عن ضخامة البيانات التي تحويها الشبكة المعلوماتية واتساع نطاقها المكاني.

وتتميز الجرائم المعلوماتية عن الجرائم التقليدية -بالإضافة إلى ما سبق- بالصفات الخاصة لمرتكب هذه الجرائم، فهو يتمتع بالذكاء في الغالب، ويمارس حياته بصورة طبيعية، من دون أن يكون هناك ما يلفت الانتباه إلى قيامه بالجريمة؛ لعدم وجود المواجهة التي تميز المجرم التقليدي. كما أن التخصص من المزايا التي يتميز بها المجرم المعلوماتي.

6. أقسام الجرائم المعلوماتية

بتتبع الكثير من الأدبيات التي تعرضت لتحديد أقسام الجرائم المعلوماتية، يتضح أنه من الصعوبة بمكان تحديد أقسام هذه الجرائم؛ نظراً إلى التغير المستمر في أنماطها وتطور التقنية الحديثة الذي يواكبه تطور في أساليب ارتكابها. وقد تم بناء التقسيم الآتي اعتماداً على طبيعة الجريمة المعلوماتية التي تتعدد محاورها وفقاً لتعدد النظرة إليها، من خلال ارتباط هذه الجريمة بوسائل التقنية الحديثة، والنظر إلى هذه الوسائل بوصفها وعاء للمعلوماتية قد يتم الاعتداء عليه مباشرة للإضرار بهذه المعلومات والتأثير فيها. ويعد هذا بذاته جريمة، أو إمكانية استخدام هذه الوسائل لارتكاب جرائم أخرى، أو استغلالها لنشر بعض الأفعال أو الأفكار التي تعد جريمة. لذا سيتم الحديث عن أقسام هذه الجرائم من خلال المحاور الآتية:

أ. الجرائم التي تستهدف النظام المعلوماتي

ويقصد بذلك الجرائم التي تستهدف معطيات الحاسوب المعنوية من برامج وتطبيقات وبيانات، والتي ترتكب من خلال برامج الحاسوب، أو عن طريق الإنترنت، وكذلك الاعتداء على بعض الأجهزة الإلكترونية الخاصة بالاتصال، ومن أهم هذه الجرائم جرائم الاختراق التي وإن كانت هي ذاتها جرائم، فإن هناك أثراً يترتب عليها ويتمثل بارتكاب جريمة أخرى؛ حيث إن المخترِق – إثر ارتكاب الاختراق- يمكن أن يقوم بارتكاب جرائم متواصلة عدة في نظام الحاسوب.[19]

ومن هذه الجرائم جريمة استخدام برامج إتلاف المعلومات التي تتنوع الطرائق الفنية والتقنية المستخدمة فيها، بدءاً من فيروسات الحاسب الآلي Programs Virus، ومروراً ببرامج الدودة Worm Software، وانتهاء بالقنبلة المنطقية أو الزمنية.[20]

ويدخل ضمن هذه الجرائم: الإغراق بالرسائل، وتعطيل الأجهزة، وكسر الشِّفرة، والتلاعب في البرامج، والتجسس على البريد الإلكتروني، وسرقة منفعة الحاسب الآلي، وقرصنة البرامج، والتعدي على برامج التطبيق والتشغيل.

ب. الجرائم التي تقع باستخدام النظام المعلوماتي

أولى هذه الجرائم: التعدي على البيانات الخاصة، ويشمل ذلك تجاوز استخدام المعلومات المجمعة عن الفرد لغرضها المقصود، والدخول

والتداول غير المرخص به للمعلومات، وكذلك الأخطاء في المعلومات والبيانات، والتشهير والإساءة إلى السمعة، والضغط والابتزاز السياسي.[21]

ويعد تسهيل جهود عصابات الجريمة المنظمة من أبرز الجرائم التي تقع باستخدام النظام المعلوماتي.

وقد كشفت باحثة بريطانية عن استغلال شبكة الإنترنت في تجارة الرقيق الأبيض، من خلال عقد صفقات لبيع الفتيات من أربعين دولة نامية، ومن أوربا الشرقية لمواطنين في دول الغرب؛ من أجل المتعة والجنس.[22]

ومن ذلك أيضاً غسل الأموال، وترويج المخدرات، وجرائم الإرهاب، والجرائم ضد الحكومة، وتهديد الأمن القومي والعسكري، والتحويل الإلكتروني، والاحتيال المعلوماتي، والقرصنة الفكرية، والتزوير المعلوماتي، والتجسس المعلوماتي، وإفشاء المعلومات، والاستخدام غير المشروع لبطاقات الائتمان، وسرقة المعلومات، والجرائم المتعلقة بالتجارة الإلكترونية.

ج. الجرائم التي تقع في بيئة النظام المعلوماتي

ويقصد بذلك الجرائم التي تتم من خلال استخدام الحاسوب أو الإنترنت؛ بوصفهما بيئة صالحة لارتكاب هذه الجرائم، عن طريق إيصالها إلى المتلقي، من دون أن يكون هناك اعتداء على النظام المعلوماتي، أو استخدامه لارتكاب جريمة أخرى.

ومن أهم هذه الجرائم: إنشاء المواقع الإباحية، واستغلال القاصرين جنسياً. وقد وفرت الإنترنت أكثر الوسائل فاعلية وجاذبية لصناعة الإباحية

ونشرها، بشتى وسائل عرضها من صور وفيديو وحوارات في متداول الجميع، وحتى الأطفال. وهذا بالطبع يعد أكبر الجوانب السلبية للإنترنت، وبخاصة في مجتمع محافظ على دينه وتقاليده كمجتمعنا العربي.[23] كما ظهرت مؤخراً جرائم خطيرة مثل التحرش الجنسي بالقاصرين عبر الحاسوب والوسائل التقنية، وتصويرهم وإظهارهم ضمن نشاطات جنسية.[24]

ومن هذه الجرائم كذلك محاولة ابتزاز بعض الأشخاص بنشر الشائعات عنهم، وتشويه سمعتهم إذا لم يرضخوا أو لم يدفعوا مقابلاً مادياً. وقد يكون الهدف هو الانتقام لأسباب مختلفة.

ويمكن أن يستخدم الحاسب الآلي والإنترنت؛ لترويج الدعارة بصورة قسرية، أو للإغواء، أو لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم، والحصول على الصور والهويات بطريقة غير مشروعة؛ لاستغلالها في نشاطات جنسية.[25] بالإضافة لما توفره الشبكة من معلومات عن بيوت الدعارة في الكثير من دول العالم، وكذلك فإن بعض المؤسسات توفر عبر هذه الشبكة أحاديث هاتفية حية، تؤديها فتيات مدربات؛ وذلك في مقابل الحصول على نسبة من عائد المكالمات التلفونية.[26]

ومن ذلك أيضاً جرائم الفتن الداخلية التي تمس الوضعية الداخلية الآمنة، والسلام الاجتماعي والاقتصادي، وهي ذات تأثير خطير في معدلات الاستقرار، حيث يمس العدوان جوانب أساسية في القيم الإنسانية في كل دولة؛ كالعنصرية وانتهاك الحقوق السياسية، ويطلق على مرتكب جرائم الفتن الداخلية مصطلح Crackpot؛ كمن يبث الفكر النازي الجديد، أو ينفث روح العداء في المجتمع.[27]

الفصل الثاني

فاعلية التشريعات العقابية في مكافحة الجرائم المعلوماتية

1. الطبيعة القانونية للجريمة المعلوماتية

يثور الآن تساؤل مهم مؤداه: ما الوضع القانوني للمعلومة؟ وقد اتجه الفقه في ذلك اتجاهين:

أ. الاتجاه التقليدي: وهو أن للمعلومات طبيعة من نوع خاص

يرتكز هذا المبدأ على بدهية، مؤداها: أن الأشياء التي توصف بالقيم هي تلك الأشياء القابلة للاستحواذ، ومؤدى ذلك أن الأشياء التي يمكن الاستئثار بها هي التي تكون من قبيل القيم، وبالنظر إلى أن للمعلومات طبيعة معنوية فإنه من غير المقبول أن تكون قابلة للاستئثار –وفقاً لهذا المنهج– إلا عن طريق حق الملكية الأدبية أو الذهنية أو الصناعية. وعلى ذلك فالمعلومة المختزنة التي لا تنتمي إلى المواد الأدبية أو الذهنية أو الصناعية، والتي تُرفض إقامتها في أي مجموعة من هذه المجموعات لا تُدرَج حتماً في مجموعة القيم المحمية. لذا حاول هذا الاتجاه أن يسوغ العقاب على أساس المنافسة غير المشروعة، بقوله: إن الخطأ لا يجد أساسه في الاستيلاء نفسه على المعلومة التي تخص الآخرين، وإنما يجد أساسه في الظروف التي اقترنت بهذا الاستيلاء، وبحيث يمكن تفادي الاعتراف بحق الاستئثار بالمعلومات.[28]

ويرى أصحاب هذا الاتجاه أن المعلومات ليس لها طبيعة مادية، فالأشياء المحسوسة هي التي تعد من قبيل الأشياء المادية، وغياب هذا الكيان

المادي للمعلومات لا يجعلها محلاً لحق مالي من نوع الحقوق المتعارف عليها في الفقه، والتي ترد حول كيانات مادية؛ لذلك يلزم بالضرورة استبعادها من طائفة الأموال.[29]

ب. الاتجاه الحديث: وهو أن المعلومات مجموعة مستحدثة من القيم

يرى هذا الاتجاه أن المعلومات ما هي إلا مجموعة مستحدثة من القيم. ويرجع الفضل في ذلك إلى الأستاذين بير كاتالا وميشيل فيفانت، حيث يذهب الأول إلى قابلية المعلومة للاستحواذ بوصفها قيمة مستقلة عن دعامتها المادية على سند من «أن المعلومة تقوَّم وفقاً لسعر السوق متى كانت غير محظورة تجارياً، وأنها منتج من دون النظر إلى دعامتها المادية وعمل من قدّمها، وأنها ترتبط بمؤلفها عن طريق رابطة قانونية، تمثَّل بعلاقة المالك بالشيء الذي يملكه، وهي تخص مؤلفها؛ بسبب علاقة التبني التي تجمع بينهما». [30]

وهكذا استند الأستاذ كاتالا إلى حجتين لإضفاء وصف القيمة على المعلومة: إحداهما قيمتها الاقتصادية، وثانيتهما علاقة التبني التي تجمع بينها وبين مؤلفها. وهاتان الحجتان لا تعدان من قبيل الحجج المألوف استعمالها من أجل الاعتراف بقيمة من القيم، ولكنهما تستحقان على أي حال كل تأييد.[31]

ويرى الأستاذ كاتالا أن المعلومات بوصفها ملكية محددة، تخول صاحبها ميزتين أساسيتين: تمثَّل الأولى في حقه في ضمان سرية المعلومة، والثانية في طلب التعويض عن الأضرار التي ترتَّب على أي عمل غير مشروع يتعلق بها. [32]

ويتفق الأستاذ فيفانت والرأي السابق، فهو يرى أن للمعلومات قيمة قابلة للتملك، لما لها من قيمة اقتصادية لا يمكن النزاع بشأنها، فهي يمكن أن تكون محلاً لعقد البيع، فالملكية الفكرية التي يحميها القانون تقوم على أساس واحد، وهو أن المعلومة قيمة من الناحية القانونية، وسواء كانت هذه المعلومة في شكل براءة اختراع، أو شكل نموذج، أو شكل مؤلف، أو كانت مجرد معلومة تنتمي لمؤلفها، فإنه يجب الاعتراف بوصف القيمة لها، وأن تصبح محلاً لحق. وينتهي الأستاذ فيفانت إلى أن ما أسماه القيمة المعلوماتية، هي حقيقةً ربما تحتاج إلى إرساء نظرية عامة بشأنها، إلا أنه ليس بالشيء المستحدث.[33]

وعلى ذلك يمكن أن تعد المعلومات مالاً قابلاً للتملك أو الاستغلال، على أساس قيمته الاقتصادية، وليس على أساس كيانه المادي؛ ولذلك فهو يستحق الحماية القانونية، ولأن البرامج في جوهرها معلومات معالجة آلياً، ولها قيمة اقتصادية؛ لذا تجب معاملتها معاملة المال.[34]

إن الفيصل في ذلك هو تحديد كلمة المادة في العلوم الطبيعية، فالمادة في العلوم الطبيعية هي كل ما يشغل حيزاً مادياً في فراغ معين، وإن هذا الحيز يمكن قياسه أو التحكم فيه؛ ومن ثم فإن البرنامج في الحاسوب يشغل حيزاً مادياً يمكن قياسه بمقياس معين هو البايت والكيلوبايت والميجابايت، وقد يؤدي هذا القول إلى أن هذه البيانات تأخذ شكل نبضات إلكترونية تمثل الرقم [صفر واحد]، وهي في هذا تشبه التيار الكهربائي الذي عده الفقه والقضاء في فرنسا ومصر من قبيل الأشياء المادية، فالمعلومات التي لا تكون متصلة بالنواحي الفنية والأدبية، ولا تشملها قوانين حماية الملكية الفنية

والفكرية، ليس من المقبول أن تظل عارية من أي حماية إذا ما جرى الاستيلاء عليها، أو استخدامها بطريقة غير مشروعة.[35]

وتبدو المعلومة – وفقاً لهذا الاتجاه – من حيث هي قيمة، ولكنها قيمة قائمة بذاتها؛ بسبب خصائص حق الملكية. ولا شك في أن لهذه الذاتية آثاراً جسيمة، سواء من الناحية المدنية أو التجارية، ولكنها لا تشكل عائقاً بالنسبة إلى انضمام القيمة المعلوماتية إلى مجموعة القيم التي يحميها قانون العقوبات.[36]

وتبدو أهمية تحديد الطبيعة القانونية للجريمة المعلوماتية في إمكانية أن تعد من ضمن الحقوق المستقلة التي تستحق الحماية القانونية؛ وذلك بسن التشريعات التي تضمن هذه الحماية، أو إمكان تكييف[37] الفعل الإجرامي المتعلق بالمعلوماتية؛ لإدخاله ضمن أفعال أخرى محمية بموجب نصوص سابقة، وتطبيقها عليه؛ وذلك وفقاً للتقسيم السابق.

وفي رأيي أن عدَّ المعلومات طائفة جديدة من القيم، وأن لها في ذاتها قيمة مالية، يتناسب وسد الفراغ التشريعي الذي يحد من مكافحة الجرائم المعلوماتية؛ لعدم إمكانية تطبيق بعض النصوص التي تجرّم بعض الأفعال التقليدية؛ اعتماداً على مبدأ الشرعية الجنائية كما سيأتي.

2. فاعلية نصوص التجريم التقليدية في مواجهة الجرائم المعلوماتية

لا يُطوَّر القانون الجنائي بالسرعة نفسها التي تُطوَّر بها التكنولوجيا أو مهارة الذهن البشري في تسخير هذه المبتكرات لاستخدام سيئ. ومن ثم فإن القانون الجنائي التقليدي لا يكفي من حيث المبدأ لمواجهة هذا الشكل الجديد

من الإجرام، ولاسيما أن النصوص التقليدية قد وضُعت لتطبّق وفقاً لمعايير معينة (منقول مادي)، على حين أن بعض القيم -في مجال المعالجة الآلية للمعلومات- لها طبيعة غير مادية؛ مثل المعلومات والمعطيات المخزنة في ذاكرة الحاسب الآلي، وكذلك حالات استخدام الجهاز من دون مقابل، يضاف إلى ذلك ما تميز به الوسائل الفنية التي تستخدم في ارتكاب هذا النوع الجديد من الجرائم من ذاتية خاصة.[38]

أما بالنسبة إلى الأغلب الأعم فإن الجرائم التقليدية التي ترتكب باستخدام الحاسب الآلي تبرز موضوعات جديدة قليلة في إطار القانون الجنائي؛ فأساس الجريمة يظل على حاله من دون النظر إلى احتمال كون الذنب قد ارتكب باستخدام الحاسوب أو بوسائل أخرى. نجد مثلاً أن التهديد بالقتل يظل تهديداً بالقتل من دون النظر إلى احتمال كونه تم بإرسال مراسلة إلكترونية بالبريد الإلكتروني أو بمكالمة هاتفية. وقد تتوافر أسباب في الظروف ذاتها؛ لتنظيم مثل هذه الجرائم بصور يختلف بعضها عن بعض، عندما ترتكب عبر الحاسوب والإنترنت. ولكن بصفة عامة نجد أن الأساس الموضوعي الذي يبرز في الجرائم التقليدية يظل قائماً، ولا يتغير إذا ما تصادف ارتكابها باستخدام الحواسيب. وأما جرائم إساءة استخدام الحاسب فإنها تبرز نوعية جديدة من الجرائم؛ ومن ثم تقوم بطرح تحديات حيوية أمام القانون الجنائي.[39]

الصعوبات التي تواجه تطبيق النصوص التقليدية

إن المعني بما ينشأ عن هذه التقنية من مخاطر وعلاقات قانونية مختلفة، في ظل الاستخدام المتزايد لتقنية المعلومات في مختلف نواحي الحياة، هو قانون

العقوبات. وهنا تثير الجرائم المعلوماتية صعوبات جمة أمام تطبيق النصوص الجنائية التقليدية المنصوصة في القوانين القائمة.

وترجع هذه الصعوبات غالباً إلى أن تلك النصوص قد وضعت أساساً؛ لحماية الأشياء المادية في مواجهة صور الاعتداء المألوفة والتقليدية. وبتعبير آخر فإن مثل هذه النصوص قد يتعذر – في ظلها – أن تقع الأفعال التي تطال المكونات غير المادية للنظم المعلوماتية تحت طائلة عقابها، أو يستحيل، إلى جانب أن جرائم المعلوماتية لها طابعها الخاص؛ نظراً لتميزها بأن هناك وسائل إجرامية مستحدثة، تستخدم أساساً لارتكاب مثل هذا النوع من الجرائم.[40]

والتطور الهائل في تكنولوجيا المعلومات والاتصالات أدى إلى ظهور سلبيات خطيرة، تهدد اقتصاد البلاد وأمنها، وهذه الجرائم تُطوَّر بسرعة هائلة؛ وهذا أوجد نوعاً من الصراع بين التقنيات والقانون؛ نتج عنه عجز هذا الأخير عن مواكبة هذا التطور السريع في ثورة المعلومات.[41]

وإدراكاً لقصور القوانين الجنائية –بما تتضمنه من نصوص التجريم التقليدية– كان لابد للكثير من الدول من أن تضع قوانين وتشريعات خاصة، أو أن تعمل على جبهة قوانينها الداخلية من أجل تعديلها، ومن أجل ضمان توفير الحماية القانونية الفاعلة ضد هذه الجرائم.[42]

3. أهمية الحماية الجنائية للمعلوماتية

إذا كان النظام المعلوماتي يحقق، من دون شك، الكثير من المزايا التي لا يمكن إنكارها، فإن استخدامه ينطوي على مخاطر لا يستهان بها. فالنظام

المعلوماتي له دواعي استخدام كثيرة أدت إلى التوسع في استخدامه؛ وذلك يفتح مجالاً جديداً للإجرام، يضع القانونيين أمام ضرورة إيجاد حلول تشريعية.

والمعلوماتية -بوصفها ظاهرة إنسانية واقتصادية واجتماعية- لا يمكن أن تطور نفسها من دون أن يتوافر لها القواعد القانونية التي تنظم استغلالها؛ نظراً إلى أنها مازالت في مرحلة التطور والتفاعل؛ وقد وضعها هذا في حيز معتم من مجالات القانون الجنائي، وبخاصة بعد ظهور الجريمة المعلوماتية والمجرم المعلوماتي.[43]

لقد أثار إجرام تقنية المعلومات تحديات لها وزنها بالنسبة إلى قانون العقوبات في كل النظم القانونية؛ حيث تأثر نتيجة لتغير نموذج الأشياء وطبيعتها من مادية إلى معنوية.

ونظراً إلى نشوء أنماط إجرامية تستهدف مصالح معترفاً بحمايتها، وتستهدف محلاً له طبيعة مغايرة لمحل الجريمة الذي عرفته قوانين العقوبات القائمة، كان من المناسب أن يتدخل المشرع الجزائي لتوفير الحماية من هذه الأنماط الخطيرة من الجرائم؛ لضمان فعالية مكافحتها، ولأن النصوص التقليدية تحكمها قواعد نظام العقاب الجزائي كما سيأتي.

القواعد التي تحكم نظام العقاب الجزائي

من المتعارف عليه أن نظام العقاب الجزائي محكوم بقاعدتين رئيسيتين:

القاعدة الأولى: مبدأ الشرعية الجنائية الموجب عدم إمكان العقاب على أي فعل من دون نص قانوني محدد.

القاعدة الثانية: قاعدة حظر القياس في النصوص التجريمية الموضوعية.[44]

وينبني على هاتين القاعدتين أن التجريم والعقاب من عمل المشرع، فالأوامر والنواهي الجنائية وجزاءاتها لا ترجع إلا إلى مصدر واحد هو القانون المكتوب، وأن القاضي لا يملك التجريم في ما لم يرد نص بتجريمه، ولا المعاقبة على أمر فرضه النص الجنائي من دون أن يقرر لمخالفته عقاباً، ولا أن يوقع عقوبة عيّنها النص من دون أن يحدد الجريمة الخاصة بها، ولا أن يقضي في جريمة بغير العقوبة المقررة لها.[45]

إن اشتراط خضوع الفعل لنص تجريم كي تكون له الصفة غير المشروعة، يعني حصر مصادر التجريم والعقاب في النصوص التشريعية، وبهذا الحق يقوم مبدأ أساسي هو مبدأ الشرعية "شرعية الجرائم والعقوبات"، ومقتضى هذا المبدأ أن الجريمة لا ينشئها إلا نص قانوني، وأن العقوبة لا يقرّرها غير نص قانوني؛ «فلا جريمة ولا عقوبة إلا بناءً على قانون».[46]

وقد أثار الفقه المعاصر موضوعاً على جانب كبير من الأهمية، يتعلق بتفاعل نظم التقنية الحديثة والقانون الجنائي، وتأثير ذلك في مبدأ الشرعية الجنائية، ولاسيما حال انعدام وجود نصوص قانونية تحكم مظاهر التقنية الحديثة، كما لاحظ الفقه –بحق في عمومه– ذلك القصور البيِّن في تعامل القانون والإنترنت خصوصاً. ومثل هذه الملاحظة تؤكد أن حداثة موضوع تعامل القانون والتقنية يعود الفضل فيها إلى الإنترنت حقاً؛ لكونها فتحت آفاقاً جديدة لم تكن موجودة من قبل.

ومع ذلك لا يُقبل أن تكون الحداثة مسوغاً لانتهاك مبدأ الشرعية، حتى في حال فرض عدم التوصل إلى الإدانة. وفي القوانين المقارنة (الأمريكية

والإنجليزية والفرنسية) مثال على ذلك، فكم من الانتهاكات حدثت عبر الإنترنت. ونتيجة عدم وجود نصوص تجرم وتعاقب، أمكن الجناة الإفلات من العقاب.[47]

لقد حاول كل من القضاء الأمريكي والقضاء الفرنسي تطبيق بعض النصوص القائمة، والخاصة بجرائم الاعتداء على الأموال على هذه النشاطات، بما يثير الجدل في شأن مدى انطباق هذه النصوص على الحالات المعروضة، وهل يعد تطبيق مثل هذه النصوص نوعاً من التوسع الذي يتعارض ومبادئ مهمة ومستقرة في القانون الجنائي؟ وهي شرعية الجرائم والعقوبات والتفسير الضيق لها.[48]

وإذا كان القضاء يلجأ أحياناً -لكي يواجه هذه الأفعال- إلى تفسير النصوص الجنائية تفسيراً من شأنه أن يوسع نطاق تطبيقها، لكي تستوعب كل ما هو جديد في المجال المعلوماتي، فإن مبدأ شرعية الجرائم والعقوبات من أهم المبادئ التي تهيمن على قانون العقوبات، وما ينجم عنه من حظر القياس في مواد التجريم والعقاب.[49]

إن حظر القياس في المواد الجنائية يؤدي إلى عدم التوسع في التفسير لإدخال الأفعال المستحدثة في نطاق النصوص الجنائية التقليدية القائمة فعلاً؛ لمواجهة خطر أفعال أخرى رأى المشرع أنها تستحق الحماية.

ضرورة المواجهة الجنائية

إذا سلّمنا أن قانون العقوبات المطبق فعلاً لا يكفي لمواجهة هذا الإجرام الجديد، فهل يعني ذلك أن نقف مكتوفي الأيدي أمام هذا الفراغ أو النقص

التشريعي؟ وهل تترك من دون عقاب أفعال إجرامية جديدة برغم خطورتها، أو تتم مخالفة مبدأ الشرعية الجنائية، بحيث يسمح للقضاء بأن يتدخل لسد هذا النقص التشريعي، أو يسارع المشرع إلى التدخل لمراجعة النصوص القائمة حتى تصبح كفيلة بحماية النظام المعلوماتي ومكافحة الإجرام الذي يتولد بسبب استخدامه أو ما يقع عليه؟ في حقيقة الأمر نجد أن المشرع الجنائي هو الوحيد الذي يتدخل كلما دعت الحاجة إلى ذلك؛ ليتناول بالتجريم والعقاب ما يستجد من أفعال لم تكن تقع من قبل تحت سلطانه؛ وذلك تطبيقاً لمبدأ الشرعية الجنائية الذي حصر مصادر التجريم والعقاب في نصوص القانون.[50]

وبما أن القانون هو الذي يحدد الجرائم، ومبدأ الشرعية الجنائية يعد من القيود التي ترد على إنزال العقاب بالمجرمين، ما لم يكن هناك نص تجريمي يسبق ارتكاب الفعل الذي يعتبر اعتداء على المصالح المحمية، فإن التجريم للأفعال المستحدثة الناتجة عن التقدم العلمي والتقنية الحديثة أمر تفرضه الحاجة الفعلية إلى ذلك، نتيجة ازدياد ارتكاب الأفعال التي تمس هذه المصالح عن طريق استخدام المعلوماتية.

وقد يكون من العوائق التي تواجه سياسة التجريم والعقاب في مجال المعلوماتية، الطبيعة الخاصة لهذه الجرائم المتمثلة في صعوبة تحديد الصفة الجرمية لها، والتي يعد أبرزها، مدى اعتبارها مالاً أو عدم اعتبارها كذلك.

الموضوع القانوني للجريمة

يقوم الموضوع القانوني للجريمة على أساس استحداث عملية ربط بين موضوعها المادي وبين المصلحة القائمة والمشروعة، التي تمثل الموضوع

القانوني للعدوان. وهذه الأخيرة، أي المصلحة، وإن كان لا يشير إليها النص الجنائي فإنها توجد في الحكمة التي توخاها المشرع من إيجاد النص؛ ليكون هذا الأخير ضامناً عدم التعدي عليها، وفي هذا الإطار فإن الفقه مستقر على أنه حيث لا مصلحة قائمة ومشروعة فلا نص جنائياً، وأن الغاية الحقيقية للقانون الجنائي إنما هي حماية المصالح القائمة والمشروعة دائماً.[51]

والرأي القائل إن القانون الجنائي لم يضع إلا لحماية أموال معينة غير سليم؛ فالصحيح أن الحماية القانونية تنصرف إلى المصلحة (القيمة) دون المال لتجعل منه مصلحة قانونية، فمحل الحماية القانونية هو المصلحة وليس المال، فقيمة المال في القانون الجنائي، والتي يسبغ عليها حمايته، لها مدلول آخر غير المدلول الاقتصادي، الذي يعرفه القانون المدني، فالقانون الجنائي ينظر إلى(القيمة) نظرة قانونية لا نظرة اقتصادية، وهي محل الحماية الجنائية.[52]

وكل جرم يمس مصلحة ما، على المشرع أن يقدر أهمية التدخل لحمايتها، والمصلحة محل الحماية في ميدان جرائم المعلوماتية هي الحق في المعلومات، من حيث هي عنصر معنوي ذو قيمة اقتصادية عالية. ويشمل ذلك الحق في الوصول إلى المعلومات، وانسيابها، وتدفقها، وتبادلها، وتنظيم استخدامها، كل ذلك على نحو مشروع من دون مساس بحقوق الآخرين في المعلومات.[53]

ومن هنا كان من الضروري أن تواكب التشريعات المختلفة هذا التطور الملحوظ في جرائم المعلوماتية؛ فالمواجهة التشريعية ضرورية للتعامل من خلال قواعد قانونية غير تقليدية مع هذا الإجرام غير التقليدي، وهي

مواجهة ينبغي أن تتعامل بشكل عصري متقدم وجرائم المعلوماتية المختلفة.[54]

الحاجة إلى تشريعات خاصة بالجرائم المعلوماتية

مما تجدر الإشارة إليه أن الجرائم المعلوماتية هي جرائم من نوع فريد، وتحتاج إلى تشريعات خاصة ووسائل مختلفة للإثبات، كما تحتاج إلى شرطة خاصة لمكافحتها، تكون مدربة بشكل نوعي على هذا النمط من الجرائم.[55]

وينطلق مفهوم الحماية القانونية عموماً من فكرة تفاعل القانون والمجتمع والبيئة الإنسانية عموماً. ذلك أن السبب المباشر لتدخل القانون محدد بعدم الاقتناع الإنساني بكفاية ظاهرة ما؛ لتنظيم ذاتها بمقتضى قوانينها الذاتية، من دون حاجة إلى اللجوء إلى القانون الوضعي، وتعني الوضعية هنا أن الدولة هي واضعة القانون وإليها ينسب، وكل سببية في تدخل القانون ينبغي أن تبنى على فكرة المصالح المهددة، تلك المصالح الحاضرة والمشروعة في النظام الاجتماعي والاقتصادي القائم. وقد يتخذ التهديد طابع العمل غير المشروع المتصف بالخطورة الخاصة التي تهدد هذه المصالح بالضرر أو بالخطر؛ فيتدخل المشرع الجنائي بالتجريم وإقرار العقاب. وهنا نكون بصدد حماية جنائية تستند إلى مبدأ الشرعية. وتعد الحماية الجنائية أشد أنواع التدخل التشريعي؛ لفرض هيمنة القانون، وحماية المصالح القائمة والمشروعة.[56]

والمعلوماتية من الظواهر الحديثة التي تمثل مصالح قائمة ومشروعة، وتستخدم في أغلب أوجه الحياة، وتمس الكثير من مناحي الحياة الإنسانية؛ لذا فهي جديرة بالحمايتين: القانونية بعامة والجنائية بخاصة، واللتين يجب أن تحيطا بكل الصور الحديثة التي أفرزتها وسائل التقنية الحديثة.

وقوانين تكنولوجيا المعلومات والاتصالات المستحدثة ينبغي تطبيقها في دول العالم كافة في آن واحد؛ ذلك أن شبكة الإنترنت على وجه الخصوص لا تعترف بالحدود بين الدول، وإذا ما أريدت المحافظة على مستوى مقبول من الحماية والأمن لها، فإن السبيل الوحيدة لضمان تحقيق أمن المنظومة المعلوماتية هي وضع استراتيجية شاملة متعددة الجوانب؛ وذلك من خلال تعاون دولي موحد، فضلاً عن ضرورة قيام الدول بإجراء تشريعات محلية وطنية وسن قوانين جديدة تعنى بمجتمع المعلومات. ولعل قانون العقوبات وقانون أصول المحاكمات الجزائية والقانون التجاري في مقدمة القوانين التي تحتاج إلى تطوير في نصوصها؛ لتمتد إلى تنظيم التعاملات الإلكترونية، وسن القوانين الجديدة، وهذا أمر ضروري لحمايتها من المخاطر والتهديدات.[57]

وتعد الجريمة المعلوماتية شكلاً جديداً من الجرائم العابرة للحدود الوطنية والإقليمية والقارية. وبعد أن صار المجتمع المعلوماتي حقيقة لا تجريداً باتت حاجته واضحة إلى قواعد جنائية موضوعية جديدة تلائم تمركز مقوماته وسائر نشاطاته حول المعلومات وتقنيتها، وتكفل مجابهة الأشكال المستحدثة للإجرام، الناشئة عن إساءة استخدام النظم المعلوماتية الحديثة، والتي أصبحت مطلباً ضرورياً من أجهزة العدالة الجنائية.[58]

4. التشريعات الدولية المتعلقة بالجرائم المعلوماتية

أ. أهمية التعاون الدولي

أدى الانتشار الواسع والمتسارع للتقنية العالية المتمثلة في الحاسبات الآلية وشبكات الاتصال الخاصة بها، والتطور الهائل في عالم البرمجيات،

وتزايد الاعتماد على بنوك المعلومات والحاسبات الآلية في تنظيم نواحي الحياة كافة، وفي البحوث العلمية والاجتماعية والثقافية، وكذلك إدارة المشروعات والتبادل التجاري وإدارة العمليات المالية والمصرفية؛ كل ذلك أدى إلى وصول هذه التقنية العالية إلى أيدي الخيِّرين والشريرين معاً؛ فاستغل بعض من يملكون المعرفة بالتقنية العالية هذه المعرفة لارتكاب الجرائم، سواء تلك الواقعة على تكنولوجيا المعلومات، أو تلك التي ترتكب بوساطة المعلوماتية.[59]

وبناء على ما سبق، أصبح من الضروري أن يكون هناك تعاون دولي واسع المدى في مكافحة الجرائم الواقعة في بيئة المعالجة الآلية للبيانات. وبرغم ضرورة هذا التعاون فإن هناك عقبات عدة تقف في سبيل تحقيقه.

أهم العقبات التي تواجه التعاون الدولي:[60]

1. عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام النظم المعلوماتية الواجب تجريمها.

2. عدم الاتفاق على مفهوم عام حول التعريف القانوني للنشاط الذي يمكن، أو يفترض، الاتفاق على تجريمه.

3. اختلاف مفاهيم الجريمة لاختلاف التقاليد القانونية وفلسفة النظم القانونية المختلفة.

4. عدم التنسيق بين قوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحري والتحقيق في الجرائم المعلوماتية.

5. نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء؛ لتمحيص عناصر ما يقع من جرائم في مجال المعالجة الآلية للبيانات وجمع المعلومات والأدلة عنها.

6. تعقد المشكلات القانونية والفنية الخاصة بتفتيش النظام المعلوماتي خارج حدود الدولة، أو ضبط معلومات مخزنة فيه، أو الأمر بتسليمها.

7. عدم وجود معاهدات للتسليم، أو التعاون الثنائي أو الجماعي بين الدول، يسمح بالتعاون الدولي أو عدم كفايتها إن وجدت؛ لمواجهة المتطلبات الخاصة للجرائم المعلوماتية ودينامية التحريات فيها، وسرعتها.

8. أن السمة الغالبة للكثير من جرائم الحاسوب من النوع العابر للحدود؛ ومن ثم فهي تثير من المشكلات الكثير مما لا تمكن السيطرة عليه.

الجهود الدولية للتغلب على العقبات السابقة

لم تمنع المعوقات السابقة مواجهة هذه الجرائم على المستوى الدولي؛ ولهذا تزايدت خطط مكافحة هذه الجرائم، وانصبت الجهود المتعمقة على دراستها، وإيجاد آليات قانونية للحماية من أخطارها، وبرز في هذا المجال المنظمات الدولية والإقليمية؛ وبخاصة المنظمات والهيئات الإقليمية الأوربية.

وقد تمت مواجهة هذه الجرائم في ثلاثة قطاعات مستقلة؛ هي: حماية استخدام الحاسوب، أو ما يعرف أحياناً بجرائم الحاسوب ذات المحتوى الاقتصادي، وحماية البيانات المتصلة بالحياة الخاصة (الخصوصية المعلوماتية)، وحماية حق المؤلف على البرامج وقواعد البيانات (الملكية الفكرية للمصنفات الرقمية)؛ وهذا نفسه أضعف إمكان صوغ نظرية عامة

للحماية الجنائية لتقنية المعلومات، وشتت الجهود بشأن إدراك كنه هذه الظاهرة، وإبداع أدوات ناجحة لمكافحتها. وهو ما أدى إلى توجه الجهود نحو صوغ نظرية عامة لجرائم الحاسوب والجرائم التي تستهدف المعلومات.[61]

ولخطورة هذه الجرائم وأهمية مكافحتها، كان من الواجب أن تتحرك الدول المختلفة في محورين:

الأول: داخلي بحيث تتواءم تشريعاتها الداخلية وهذا النمط الجديد من الجرائم.

والثاني: دولي عن طريق عقد الاتفاقيات الدولية؛ حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية أولاً، وغياب الاتفاقيات الدولية التي تعالج سبل مواجهة هذه الجرائم ثانياً.[62]

ب. جهود هيئة الأمم المتحدة

يبرز اهتمام هيئة الأمم المتحدة بالجرائم المعلوماتية من خلال ما دعت إليه الجمعية العامة في فقرتها الثالثة من منطوق قرارها 56/ 19 بتاريخ 29 تشرين الثاني/ نوفمبر 2001؛ بشأن التطورات في ميدان المعلومات والاتصالات؛ حيث توجهت إلى جميع الدول الأعضاء بضرورة مواصلة إبلاغ الأمين العام بأدائها وتقوياتها بشأن ما يأتي:

1. التقويم العام لمسائل أمن المعلومات.
2. تحديد المفاهيم الأساسية المتعلقة بأمن المعلومات.

3. مضمون المفاهيم الدولية ذات الصلة الرامية إلى تعزيز أمن النظم العالمية للمعلومات والاتصالات.

وقد دعت الفقرة الرابعة من قرار الأمين العام للأمم المتحدة إلى دراسة الأخطار القائمة والمحتملة لأمن المعلومات، وإعداد التدابير التعاونية التي يمكن اتخاذها للتصدي لتلك الأخطار، وأن تجرى دراسة بمساعدة فريق الخبراء الحكوميين الذي تم إنشاؤه عام 2004، وتولى الأمين العام تعيين أعضائه على أساس التوزيع الجغرافي العادل، بالتعاون والدول الأعضاء القادرة على تقديم تلك المساعدة.[63]

وفي هذا المجال أُصدرت قرارات ونظمت مؤتمرات دولية وإقليمية عدة؛ من ذلك مثلاً: قرارا الجمعية العامة للأمم المتحدة 6355/ و12156 بشأن مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، وبروتوكول حماية الأطفال على الإنترنت 2002، وإعلان فيينا بشأن الجريمة والعدالة (مواجهة تحديات القرن الحادي العشرين) عام 2000، وقرار مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء (هافانا 1990)،[64] والقمة العالمية لمجتمع المعلومات 2005، وقرار المؤتمر العالمي لتنمية الاتصالات رقم 45 (الدوحة، 2006)، والقواعد الإرشادية لمنظمة التعاون الاقتصادي والتنمية (OECD).

ج. المعاهدات والاتفاقيات والمؤتمرات الدولية

* الاتفاقية الأوربية لمكافحة جرائم الحاسب الآلي.

شهدت العاصمة المجرية بودابست أواخر عام 2001 صدور التقرير النهائي حول المعاهدات الدولية التي تكافح جرائم الإنترنت، وتبلور التعاون والتضامن الدولي في محاربتها، ومحاولة الحد منها، وخاصة بعد أن وصلت تلك الجرائم إلى حد خطير، أصبح يهدد الأشخاص والممتلكات. وتتكون هذه الاتفاقية من ثمان وأربعين مادة، موزعة على أربعة أبواب، يعالج الباب الأول منها استخدام المصطلحات، ويتناول الثاني الإجراءات الواجب اتخاذها على المستوى القومي، ويضم ثلاثة أقسام: أولها للقانون العقابي المادي أو الموضوعي، وثانيها للقانون الإجرائي، وثالثها للاختصاص القضائي.[65]

* توصيات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات عام 1994.

* اتفاقية المجلس الأوربي لحماية الخصوصية والسرية عام 1968.

* إعلان القاهرة (الوثيقة العربية نحو مجتمع معلومات عربي)، 8 حزيران/ يونيو 2003.

5. التشريعات المحلية المتعلقة بالجرائم المعلوماتية

تباينت اتجاهات الدول المختلفة في التعامل وظاهرة الجريمة المعلوماتية، ويمكن بصفة عامة التمييز بين اتجاهين رئيسيين في هذا الخصوص:[66]

الاتجاه الأول: يذهب إلى النظر إلى الجرائم المرتبطة بالحاسبات الآلية؛ من حيث هي جرائم عادية، لا تتصف بخصائص تميزها من غيرها من الجرائم، بحيث تتطلب نصوصاً خاصة لمواجهتها.

الاتجاه الثاني: ويذهب عكس الأول، بحيث يرى ضرورة التدخل التشريعي لمواجهة الجريمة المعلوماتية؛ نظراً إلى ما تتميز به من سمات تميزها من غيرها من الجرائم، ويظهر هذا التدخل التشريعي في إيجاد نصوص جديدة، يضاف إليها البعد الخاص بالحاسب الآلي، أو تعديل بعض النصوص القائمة.

الأساليب والأنماط المختلفة للصياغات التشريعية المختلفة

تختلف الأساليب التي تلجأ إليها التشريعات في الدول المختلفة بصوغ نصوص الحماية الجنائية لنظم المعلومات، ويمكن أن نقول إن هناك أنماطاً تشريعية عدة قد يلجأ إليها المشرع في هذا الصدد، مع إمكانية الجمع بينهما. ويمكن إيجاز هذه الأنماط أو الأساليب التشريعية فيما يأتي:[67]

1. الإضافة Supplementation: تتجه بعض الدول إلى أن تضيف إلى النصوص القائمة بالفعل تلك الحالات التي يرتكب فيها الجاني النشاط الإجرامي الوارد بها، بوساطة الحاسب الآلي، أو أن تضيف إلى محل السلوك الإجرامي الوارد في النصوص القائمة المعلومات التي يحويها نظام الحاسب الآلي؛ مثل عدِّها محلاً يتم السطو عليه، كما في نصوص جريمة السرقة.

2. وضع نصوص جديدة قياساً على نصوص تقليدية قائمة بالفعل Extention: ففي هذه الحالة يصاغ نص جديد يتفق وأحد الأشكال التقليدية للسلوك الإجرامي؛ حيث تم تحويل السلوك من صورته التقليدية إلى صور أخرى، ترتبط بالحاسب الآلي ونظامه؛ بوصفهما المحل الجديد للسلوك الإجرامي، وعادة ما يتبع أغلب الدول هذه الطريقة.

3. تتجه بعض الدول إلى وضع نص رئيسي واحد يستطيع التعامل والأوجه المختلفة للجريمة المعلوماتية "One-for-all"، (الولايات المتحدة الأمريكية)، أو تجميع كل ما يتعلق بالجريمة المعلوماتية في قسم مستقل ملحق بالتشريع الجنائي، أو في تشريع مستقل، وتوضح كلتا الطريقتين الطبيعة الخاصة للجريمة المعلوماتية، كما تسمح بوضع عقوبات خاصة لهذه الجريمة بحيث تتلاءم وإياها.

4. وأخيراً فإن الجمع بين أكثر من نمط من هذه الأنماط أمر وارد، والحقيقة أن اختيار أي طريقة من هذه الطرائق يتأثر كثيراً بالوقت الذي تدخل فيه المشرع لمواجهة الجريمة المعلوماتية، وكذلك طبيعة النظام القانوني في كل دولة.

ولتأكيد أهمية الحماية القانونية للمعلومات، سعى الكثير من دول العالم إلى إصدار قوانين خاصة، تعنى بجميع الأفعال التي ترتكب من خلال النظام المعلوماتي، أو التي تقع عليه، أو تمارس في بيئته؛ لمواجهة خطر تلك الأفعال والحد من ارتكابها، كما قام بعض الدول بتعديل قوانينها أو الإضافة إليها للغرض نفسه، وذلك على النحو الآتي:

أولاً: على المستوى العالمي

أمام الخصائص المميزة لجرائم الحاسوب، وأمام مشكلاتها وتحدياتها المتزايدة، وأمام اتجاهات العمل الدولي العالمي والإقليمي بشأن سياسات مكافحتها، اتجه عدد من الدول، في مقدمتهم الولايات المتحدة الأمريكية

ودول أوربا إلى وضع تشريعات خاصة، أو تعديل قوانين العقوبات لديها؛ بغية تجريم جرائم الحاسوب والإنترنت. وقد جاء اتجاه التشريع المقارن في التعامل وجرائم الحاسوب متفقاً والاتجاهات ذاتها التي سنتها المنظمات الإقليمية والدولية.[68]

وتعد السويد من أوائل الدول التي اتجهت إلى سن تشريعات قانونية جديدة خاصة بجرائم الإنترنت والحاسب الآلي؛ لتستطيع معاقبة المتهمين بارتكاب الجرائم الإلكترونية؛ حيث صدر أول قانون خاص بها سمي "قانون البيانات"، وقد صدر هذا القانون عام 1973. وفي الولايات المتحدة جرمت بعض القوانين الاستعمال غير المصرح به لنظام الحاسب الآلي، ومن ذلك القانون الخاص بجرائم الحاسبات الآلية في فرجينيا الصادر عام 1986؛ حيث تضمن القانون نصاً يجرم سرقة الخدمات التي يقدمها الحاسب الآلي، ومُيِّز هذا النص بتطلبه أن يكون الاستعمال قد تم بسوء نية، متفادياً الانتقادات التي وجهت إلى مشروع القانون الفيدرالي لحماية نظم الحاسبات الآلية 1977– 1979، وإلى قوانين الولايات التي تأثرت به في نصوصها؛ حيث كان يقضي بمعاقبة كل من يستخدم عمداً أحد نظم الحاسبات الآلية من دون أن يكون مصرحاً له بذلك. على حين جاء هذا النص بتطلبه أن يكون الاستعمال قد تم بسوء نية؛ ليستبعد من نطاقه الاستعمال المجرد لنظام الحاسب الآلي. ويرى بعض المختصين أن القانون الخاص بجرائم الحاسبات الآلية في ولاية كاليفورنيا لعام 1985 قد سلك الاتجاه نفسه، من حيث ابتعاده عن تجريم الاستعمال غير المصرح به لنظام الحاسب الآلي بعامة. وسلكت بعض الولايات مسلكاً مغايراً في تجريم الاستعمال غير المصرح به لنظام

الحاسب الآلي؛ حيث تطلب لتجريمه أن تتجاوز قيمة الخدمات التي يحصل عليها الفاعل نتيجة هذا الاستعمال حداً معيناً، وإلا فسوف تنفى عن الفعل الصفة غير المشروعة.

أما على المستوى الفيدرالي فكان هناك اقتراح بإضافة نص لتجريم الاستعمال غير المصرح به لنظام الحاسب الآلي إلى القانون الفيدرالي لجرائم الحاسبات الآلية لعام 1984؛ وذلك عن طريق إضافة الخدمات التي يقدمها الحاسب الآلي، بحيث يشملها تعريف الممتلكات التي يحميها هذا القانون.[69] وقد أطلق عليه قانون الاحتيال وإساءة استخدام الحاسب الآلي، وتم تعديله مرتين، عامي 1986 و 1994. [70]

وقد انضمت الولايات المتحدة إلى اتفاقية مجلس أوربا الخاصة بالجرائم السيبرانية، وصدق عليها الرئيس الأمريكي في 22 أيلول/ سبتمبر 2006، لتدخل حيز النفاذ في 1 كانون الثاني/ يناير 2007. وكان الرئيس بوش قد طلب إلى مجلس الشيوخ إقرار الاتفاقية التي تفرض على الأطراف فيها أن تعد الأفعال التي يتم ارتكابها من خلال أجهزة الحاسوب أو ضدها، أو تلك المتصلة بها، جرائم يعاقب عليها القانون.[71]

ولا توجد تشريعات مكتوبة بالمملكة المتحدة تعالج ظاهرة الجرائم المعلوماتية. ويرجع السبب في ذلك إلى أن النظام القانوني البريطاني يعتمد بصفة أساسية على السوابق القضائية، غير أنه صدر قانون إساءة استخدام الحاسوب فيها عام 1990، الذي تناول المسؤولية الجنائية للجرائم المعلوماتية من خلال القسم الثامن عشر[72] بثلاثة بنود هي:[73]

1. الدخول المحظور على مواد الحاسوب.

2. الدخول المحظور بقصد التسهيل والتحريض على الجرائم.

3. حظر تبديل مواد الحاسوب أو تحويلها.

وقد عدلت المملكة المتحدة، بجهود البرلمان الإنجليزي تحديداً، قانون حق المؤلف، الذي صدر عام 1956؛ ليشمل بقائمته الخاصة المصنفات الخاضعة لحماية برامج الحاسب الآلي.[74]

ويختلف الوضع بالنسبة إلى فرنسا فلم تصدر تشريعات خاصة بالحاسب الآلي، بل تضمن قانون العقوبات الفرنسي والتعديلات المتلاحقة عليه، إضافة نصوص خاصة بالمعالجة الآلية للبيانات والمعلومات. ويعد قانون العقوبات الفرنسي رقم (19– 88) الصادر عام 1988 أول تشريع فرنسي لتجريم بعض صور جرائم الحاسب الآلي، والذي جرّم الدخول إلى نظام المعالجة الآلية للمعلومات، أو البقاء فيه بطريق غير مشروعة.[75] واستمر العمل بهذا القانون إلى أن صدر تعديله عام 1994؛ رغبة من المشرع الفرنسي في الحد من الظاهرة الإجرامية، وكان مقتضى ذلك التعديل إضافة فصل ثالث إلى الباب الثاني من القسم الثالث من قانون العقوبات، تحت عنوان "الاعتداءات على نظم المعالجة الآلية للمعلومات".[76]

كما أصدرت فرنسا القانون رقم 660/ 85 في تاريخ 3/ 6/ 1985، الذي تم بموجبه إضافة فقرة جديدة إلى قائمة المصنفات الواردة في قانون حق المؤلف، مع إفراد مدة حماية خاصة ببرامج الحاسب الآلي بلغت25 سنة، تبدأ بتاريخ الانتهاء من العمل.[77]

وفي النمسا صدر تشريع خاص للمعلومات عام 2000، وفي العام نفسه عدلت بلجيكا المادة رقم 550 ب من القانون الجنائي؛ ليشمل المشكلات الرئيسية المتعلقة بالمعلوماتية. كما أقر القانون البرازيلي في العام نفسه بعض شروط عقاب إخفاء البيانات المزورة وإدخالها في نظام المعلومات. وفي جمهورية التشيك طبقت قواعد القانون الجنائي القائم على الجرائم المعلوماتية من خلال مواد محددة.

كما صدرت تعديلات وإضافات مشابهة في كل من أستونيا وفنلندا وألمانيا واليونان والمجر وإيطاليا والمكسيك وهولندا. وفي اليابان صدر قانون حظر الدخول إلى الحاسوب عام 1999. [78]

ومن الدول التي وضعت قوانين خاصة لبرامج الحاسوب كوريا الجنوبية؛ حيث أصدرت قانوناً خاصاً لبرامج الحاسب الآلي، وهو القانون الذي صدر عام 1986 ويسمى "قانون حماية برامج الحاسب الآلي"، ضمن الإطار العام لمبادئ حق المؤلف، كما أصدرت الدنمارك قانوناً بهذا الخصوص هو "قانون جرائم الحاسب الآلي" عام 1985. [79]

كما صدرت تشريعات مشابهة في كل من أستراليا وهونج كونج وأيرلندا وأيسلندا والهند ولكسمبورج ومالطا والنرويج وبولندا والبرتغال وسنغافورة وجنوب أفريقيا وإسبانيا وسويسرا وتركيا.[80]

وجميع التشريعات السابقة أُجريت عن طريق الإضافة أو التعديل للقوانين القائمة، أو تجميع النصوص المتعلقة بالتجريم في باب واحد.

وتهدف جميعاً إلى مواجهة خطر الجرائم المعلوماتية الذي بات يهدد الأمن بأبعاده كافة، من خلال استخدام النظام المعلوماتي في ارتكاب بعض الجرائم التقليدية أو الجرائم المستحدثة.

ويلاحظ أن الاهتمام بالجرائم المعلوماتية يرتبط بالمستوى الحضاري والتقدم التقني للدول، وأن جميع التشريعات الدولية والوطنية السابقة تم سنها في الدول المتقدمة؛ لإحساسها بخطورة هذه الجرائم على أمن التعاملات الإلكترونية التي أصبحت من المقومات الرئيسية في جميع المجالات.

الاتجاهات العامة للقانون المقارن بشأن جرائم الحاسوب

إن التتبع الأولي لنصوص التشريعات الخاصة أو نصوص القوانين المعدلة لقوانين العقوبات، والخاصة بمواجهة ظاهرة جرائم الحاسوب، يظهر لنا الحقائق الآتية:[81]

1. تفاوت هذه التشريعات في تحديد الأنماط الجرمية الجديدة، ونص تجريمها وعقابها، لكنها في مجموعها لا تخرج على نطاق الحد الأدنى الذي بيناه لهذه الجرائم، لدى استعراض جهود المنظمات الإقليمية والدولية.

2. تحدد النصوص التي انطوت عليها التشريعات المقارنة، بشأن جرائم الحاسوب محل الاعتداء، بمعطيات الحاسوب بمدلولها التقني الواسع، سواء ارتكب الفعل عليها مباشرة أو استخدمت لتسهيل ارتكاب فعل

آخر، وأساس التجريم الاعتداء على المعطيات، لا وصف الفعل الذي سهل بشكل أدق استخدام الحاسوب، أو معطيات الحاسوب لارتكابه.

3. اتجاه الكثير من النظم القانونية المقارنة نحو إضافة صور التجريم الجديدة إلى نصوص القسم الخاص من قوانين العقوبات في نظمها القانونية، وفي ذلك إقرار بانطباق الأحكام العامة عليها أولاً، وتفضيل لآلية ضم هذه الجرائم إلى قانون العقوبات بدلاً من إفراد قوانين خاصة بذلك ثانياً، ونجد هذا المسلك قد تبنته توصيات المؤتمر السادس للجمعية المصرية للقانون الجنائي. ولكن هذا ليس الاتجاه الوحيد؛ فقد اتجه الكثير من الدول إلى إفراد قوانين خاصة، تنظم مسائل جرائم الحاسوب والإنترنت، كما في القانون الأمريكي والقانون البريطاني وغيرهما؛ حيث أفردت قوانين خاصة بجرائم الحاسوب.

4. إجماع العقوبات التي قررتها هذه القوانين، في أغلبها بين نموذج العقوبات المانعة للحرية ونموذج العقوبات المالية؛ لأثرهما مجتمعين في مواجهة مخاطر هذه الجرائم وخسائرها، كما أن بعض القوانين، كالفرنسي مثلاً، نص عقوبات تكميلية تتمثل بمصادرة الأجهزة المستخدمة في الجريمة. وهذا مسلك حسن؛ لأثره الشخصي (في نفسية الفاعل) وأثره الموضوعي في فعالية مواجهة هذا النوع من الجرائم.

5. أظهر الصوغ الفني لنصوص التجريم في القوانين المقارنة بشأن جرائم الحاسوب مراعاة الجوانب التقنية (التوصل بالنظام، والبقاء في النظام، والاختراق، والمحو والتعديل، والمعالجة الآلية وغير ذلك)، كما يبتعد

الصوغ من حيث استخدام المصطلحات القانونية الدالة على الجرائم عن المصطلحات التقليدية في أغلبه. والمستخدم من المصطلحات التقليدية (مثل: الاحتيال، أو الغش، أو الإتلاف، أو الاستيلاء، أو السرقة في جريمة سرقة وقت الحاسب فقط) يتخذ مدلولات تختلف في جوانب كثيرة عن مدلولاتها التقليدية.

ثانياً: على المستوى العربي

لعل أبرز ما يمكن أن يقال عن الجهود العربية المبذولة من أجل الحماية من جرائم الحاسب الآلي، اعتماد مجلس وزراء الداخلية العرب القانون الجزائي العربي الموحد قانوناً نموذجياً، بموجب القرار رقم 229 لسنة 1996، الذي احتوى على فصل خاص بالاعتداء على حقوق الأشخاص، وهو مستخلص من الجذاذات والمعالجات المعلوماتية في المواد 461 – 464؛ حيث أشارت المواد 461 – 463 إلى وجوب حماية الحياة الخاصة، وأسرار الأفراد من خطر المعالجة الآلية، وإلى كيفية جمع المعلومات الاسمية، وكيفية الاطلاع عليها. أما المادة 464 فقد نصت عقاب من يقوم بفعل الدخول، بطريق الغش إلى نظام المعالجة الآلية للمعلومات كله أو إلى جزء منه، وعرقلة نظام التشغيل عن أداء وظائفه المعتادة أو إفساده، وتغيير المعلومات داخل النظام، وتزوير وثائق المعالجة الآلية وسرقة المعلومات.[82]

وقد ورد في مسودة عمل الاستراتيجية العربية للاتصالات والمعلومات (بناء مجتمع المعلومات 2007 – 2015): «**المحور الرابع: بناء الثقة والأمن في استعمال الاتصالات وتكنولوجيا المعلومات**».[83]

إن تعزيز إطار الطمأنينة الذي يشمل أمن المعلومات والشبكات وحماية البيانات والخصوصية شرط أساسي لا غنى عنه لتنمية مجتمع المعلومات، وبناء الثقة بين مستخدمي أدوات تكنولوجيا الاتصالات والمعلومات وتطبيقاتها، وفى هذا المجال يتعين إيلاء ما يأتي اهتماماً خاصاً:

أ. الجرائم السيبرانية وإساءة استعمال تكنولوجيا الاتصالات والمعلومات.

- العمل إقليمياً على منع الجرائم السيبرانية، واكتشافها ومواجهتها، ومنع إساءة استعمال تكنولوجيا الاتصالات والمعلومات؛ وذلك عن طريق وضع خطوط توجيهية، تدعم الجهود الحالية في هذه المجالات، والنظر في سن تشريعات تسمح بالتدخل الفعال، عند الحاجة إلى ذلك.

ب. تشريعات حماية البيانات والخصوصية.

- التأكد من أن التشريعات القائمة تحمي المستهلك، وتضمن حماية البيانات والخصوصية، عند استخدام تكنولوجيا المعلومات والاتصالات.

جـ. أمن المعلومات والشبكات.

- دعم العمل الإقليمي والوطني، والتنسيق المستمر واتخاذ الإجراءات الفعالة كافة؛ من أجل دعم أمن المعلومات والشبكات وحمايتها.

أما عن الحال في الدول العربية منفردة، فإنه لا توجد قوانين خاصة بالجرائم المعلوماتية، وإنما يتم التعامل وهذه الجرائم بموجب قواعد القوانين التقليدية التي تفرض بعض الحماية ضد الأفعال المشابهة، بحيث يمكن تطبيق النصوص القائمة وتطويعها لمعالجة بعض أنواع الجرائم المعلوماتية، أو اللجوء إلى قوانين حماية الملكية الفكرية لحماية البرامج والبيانات؛ بوصفها مصنفات فنية.

وتعد نصوص التجريم المقررة في قوانين العقوبات العربية عاجزة عن مواجهة خطر جرائم الحاسوب؛ ونقصد هنا خطر الجرائم الواقعة على البيانات المالية، أو المتعلقة بالذمة المالية، فإذا ما أضيف إلى هذا الواقع عدم وجود نصوص تجرم أفعال الاعتداء على البيانات الشخصية المخزنة في نظم المعلومات وبنوكها، أو نصوص تحمي البيانات من خطر المعالجة الآلية، وتكفل حماية الخصوصية، بوجه عام طبعاً وفي جميع الدول العربية، فإننا نكون أمام واقع قاتم لن تزيل قتامته إلا جهود وتدابير تشريعية حثيثة لسد النقص الحاصل، وإيجاد قواعد تحيط بهذا النمط الخطر والمستجد من أنماط الإجرام.[84]

وتبرز الدول الخليجية في مجال مواجهة الجرائم المعلوماتية؛ إذ يعد القانون العُماني أول قانون عربي يتطرق إلى مواجهة هذه الجرائم، من خلال التعديل الذي تم على قانون الجزاء العُماني رقم 7 الذي صدر عام 1974، بموجب المرسوم السلطاني رقم 72/ 2001. ومن ضمن هذه التعديلات إضافة الفصل الثاني مكرر إلى الباب السابع تحت عنوان جرائم الحاسب الآلي، ويعد هذا القانون باكورة القوانين العربية في مجال مواجهة الجرائم المعلوماتية، من خلال تعديل قانون العقوبات.

وتعد دولة الإمارات العربية المتحدة أول دولة عربية تصدر قانوناً مختصاً في مكافحة جرائم المعلومات؛ فقد أصدر صاحب السمو الشيخ خليفة بن زايد آل نهيان رئيس الدولة، القانون الاتحادي رقم 2 لسنة 2006، في شأن مكافحة جرائم تقنية المعلومات، ويعد هذا القانون من القوانين النموذجية التي تناولت أغلب الجرائم المعلوماتية. وهو أول قانون في الدول العربية يصدر بشكل مستقل لمواجهة الجرائم المعلوماتية.

وفي المملكة العربية السعودية صدر نظام مكافحة الجرائم المعلوماتية بالمرسوم الملكي رقم (م17) في تاريخ 7/ 3/ 1428هـ، الذي يهدف إلى مواجهة جرائم الحاسب الآلي والإنترنت، من خلال وضع آلية نظامية للحد من وقوع هذا النوع من الجرائم؛ وذلك بتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة، وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات؛ بما يؤدي إلى تحقيق الأمن المعلوماتي، وزيادة استخدامات الحاسب وشبكاته، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات والشبكات، وحماية المصلحة العامة والأخلاق والآداب العامة.

الفصل الثالث

التشريعات الخليجية لمكافحة الجرائم المعلوماتية

1. الحماية النظامية والقانونية للمعلومات في دول مجلس التعاون

تبدأ الحماية النظامية والقانونية غالباً من نصوص الدساتير وخاصة حماية وسائل الاتصال، التي تعد من العوامل المهمة لعمل وسائل التقنية الحديثة، وعلى وجه الخصوص الشبكة العالمية (الإنترنت).

كما سلكت دول الخليج مسلك أغلب دول العالم في حماية المعلومات، عن طريق قوانين حقوق الملكية الفكرية، بحيث تمتد حماية هذه القوانين؛ لتشمل برامج الحاسب الآلي وتطبيقاته، قبل أن تتوجه بعض دول الخليج إلى إصدار نظم وقوانين خاصة بالجرائم المعلوماتية.

ونتطرق هنا إلى أوجه الحماية التي تتمثل بالحماية النظامية، أو الحماية القانونية التي وردت ضمن نظم غير جنائية، ثم الحماية الجنائية من خلال النظام الجنائي أو القانون الجنائي (القسم الخاص)، في كل دولة وحدها:

الحماية النظامية في المملكة العربية السعودية

1. الحماية الدستورية

إيماناً من الدولة بأهمية وسائل الاتصال والاعتماد عليها في التعاملات الحكومية والفردية، ولتعلقها بالأسرار الحكومية المتعلقة بأمن الدولة ومرافقها العامة، وبأسرار الفرد وحقوقه الخاصة فقد نص النظام الأساسي للحكم[85] حظر مصادرتها أو تأخيرها أو الاطلاع عليها أو الاستماع إليها؛ وذلك من خلال المادة الأربعين التي نصت أن «المراسلات البرقية والبريدية والمخابرات الهاتفية وغيرها من وسائل الاتصال مصونة، ولا يجوز مصادرتها أو تأخيرها أو الاطلاع عليها أو الاستماع إليها إلا في الحالات التي يبينها النظام».

2. الحماية عن طريق نظام الاتصالات

صدر نظام الاتصالات بالمرسوم الملكي رقم (م/ 12)، بتاريخ 12/ 3/ 1422هـ.[86]

أبرز ما ورد في هذا النظام بخصوص حماية النظام المعلوماتي، المادة التاسعة التي نصت أن «سرية المكالمات الهاتفية والمعلومات التي يتم إرسالها أو استقبالها عن طريق شبكات الاتصالات العامة مصونة، ولا يجوز الاطلاع عليها أو الاستماع إليها أو تسجيلها إلا في الحالات التي تبينها النظم».

ونظراً إلى تطور وسائل الاتصال والحاجة إلى مواكبة الحماية لهذا التطور، صدر قرار مجلس الوزراء رقم (20) بتاريخ 16 / 1 / 1426هـ؛ لتحقيق الحماية، والحد من الاختراقات عبر شبكة الإنترنت. وقد تضمن القرار: الموافقة على إضافة فقرة جديدة تحمل الرقم (14) إلى المادة السابعة والثلاثين من نظام الاتصالات، الصادر بالمرسوم الملكي رقم (م/ 12) بتاريخ 12/ 3/ 1422هـ، بالنص الآتي: «14- إلحاق ضرر بشبكات الاتصالات وتقنية المعلومات العامة، أو التعدي عليها، أو قطعها، سواء بغرض الاستفادة غير المشروعة منها، أو تعطيل الاتصالات، أو منع تبادل المعلومات بشكل عام». ويعاد ترتيب بقية فقرات المادة تبعاً لذلك. وقد أعد مشروع مرسوم ملكي بذلك، صيغته مرافقة لهذا.[87]

3. الحماية عن طريق نظام المطبوعات والنشر

تضمن نظام المطبوعات والنشر الصادر بالمرسوم الملكي رقم (م/ 32)، بتاريخ 3/ 9/ 1421 هـ النص على حماية برامج الحاسب الآلي، من خلال المادة الثانية التي نصت أن تخضع لأحكام هذا النظام النشاطات الآتية:

وذكر المنظِّم من ضمن هذه النشاطات في الفقرة السابعة عشرة إنتاج برامج الحاسب الآلي أو بيعها أو تأجيرها.

وقد تضمن النظام العقوبة المترتبة على مخالفة أحكام هذا النظام من خلال المادة الثامنة والثلاثين التي نصت أنه «مع عدم الإخلال بأي عقوبة أشد ينصها نظام آخر، يعاقب كل من يخالف حكماً من أحكام هذا النظام بغرامة مالية لا تتجاوز خمسين ألف ريال، أو بإغلاق محله أو مؤسسته مدة لا تتجاوز شهرين، أو بإغلاق محله أو مؤسسته نهائياً، ويصدر بالعقوبة قرار من الوزير بناء على اقتراح اللجنة المنصوصة في المادة السابعة والثلاثين من هذا النظام.

ويلاحظ أن هذا النظام نص نصاً صريحاً على برامج الحاسب الآلي وعلى أوعية المعلومات؛ وهذا يعد وسيلة من وسائل الحماية النظامية التي تهدف إلى حماية النظام المعلوماتي بشكل عام.

4. الحماية عن طريق نظام حماية حقوق المؤلف

صدر نظام حماية حقوق المؤلف بالمرسوم الملكي(م / 41) بتاريخ 2/ 7/ 1424 هـ؛[88] ليحل هذا النظام محل نظام حماية حقوق المؤلَّف، الصادر بالمرسوم الملكي رقم (م/ 11) بتاريخ 19/ 5/ 1410 هـ. وقد حدد النظام المصنفات المتمتعة بالحماية، من خلال المادة الثانية في الفصل الأول، التي حددت المصنفات الأصلية، ومن ضمنها الفقرة الحادية عشرة التي نصت على برمجيات الحاسب الآلي. كما حدد المنظم عقوبات معينة لكل من يخالف حكماً من أحكام النظام.

وقد ورد في المادة العاشرة من اللائحة التنفيذية لنظام حقوق المؤلف، التي اعتمدها وزير الثقافة والإعلام: "حماية قواعد البيانات"، حيث نص

أن تتمتع بالحماية قواعد البيانات الأصلية؛ بفضل انتقاء محتوياتها وترتيبها، من حيث هي إبداعات ذهنية، ولا تمتد هذه الحماية إلى البيانات أو المواد ذاتها.

وقد تضمنت المادة السادسة عشرة الاعتداء على برامج الحاسب الآلي؛ وذلك على النحو الآتي:

أ. تتمتع برامج الحاسب الآلي وبرامج ألعاب الحاسب بالحماية، سواء كانت بلغة المصدر أو بلغة الآلة؛ بوصفها أعمالاً أدبية.

ب. يعد تعدياً على حق المؤلف كل استخدام للبرامج يخالف الاستخدامات التي يحددها صاحب الحق؛ مثل:

- استنساخ البرامج وبرامج الألعاب.
- تأجير البرامج أو برامج الألعاب، أو الترخيص بالاستخدام الجماعي لها، من دون وجود وثائق تخول المؤجر ممارسة هذا الحق، بعد موافقة الوزارة عليه.
- تحميل الشبكات الداخلية أو الأجهزة برامج مستنسخة.

ومما سبق يتضح أن المملكة من الدول التي أسبغت الحماية على برامج الحاسب الآلي، من خلال حماية حقوق المؤلف؛ بوصفها من المصنفات التي تخضع للحماية، بوساطة هذا النظام. ويلاحظ أن العقوبات المحددة تتعلق بالمخالفات التي ترتكب خلافاً لأحكام النظام، وتصدرها لجنة شبه قضائية.

الحماية القانونية في دولة الإمارات العربية المتحدة

1. الحماية الدستورية

نصت المادة (31) من دستور دولة الإمارات العربية المتحدة لعام 1996، الذي صدر تعديلاً للدستور المؤقت لعام 1971 أن حرية المراسلات البريدية والبرقية وغيرها من وسائل الاتصال، وسريتها مكفولتان وفقاً للقانون.

2. الحماية عن طريق قانون حماية المصنفات الفكرية وحقوق المؤلف

صدر القانون الاتحادي رقم (40) لسنة 1992؛ في شأن المصنفات الفكرية وحقوق المؤلف، وقد شمل هذا القانون برامج الحاسب الآلي بالحماية، من خلال ما ورد في الباب الأول من المادة الثانية الفقرة 2/ ز، التي نصت أن تشمل الحماية المصنفات الفكرية الآتية؛ وذكر منها: «المصنفات السينمائية والتلفزيونية والإذاعية، والأعمال الابتكارية السمعية والبصرية، وبرامج الحاسوب».

العقوبات

يلاحظ أن المشرع الإماراتي في هذا القانون عدَّ مخالفة نصوص الحماية الفكرية لبرامج الحاسب الآلي جرائم يعاقب عليها القانون بعقوبة جنائية، على عكس النظام السعودي الذي عدَّ هذه العقوبات لقاء مخالفة أحكام النظام، ولم يذكر مسمى جريمة.

وقد حدد المشرع الإماراتي العقوبات الآتية:

أ. العقوبات الأصلية

- **المادة (38)**: «يعاقب بالحبس وبالغرامة التي لا تقل عن (50000) خمسين ألف درهم، أو بإحدى هاتين العقوبتين، من قام بنشر مصنف غير مملوك له، من دون الحصول على إذن كتابي من مؤلف المصنف أو ورثته أو من يمثله، ويعاقب بالعقوبة ذاتها من يدعي على خلاف الحقيقة أنه مالك مصنف من المصنفات».

- **المادة (39)**: «يعاقب الناشر الذي يتولى نشر مصنف من المصنفات بالحبس وبالغرامة التي لا تقل عن (10000) عشرة آلاف درهم، أو بإحدى هاتين العقوبتين؛ إذا عدل عند النشر في حقيقة المصنف وطبيعته وموضوعه وعنوانه، مخالفاً بذلك تعليمات مؤلف المصنف ورغبته».

- **المادة (40)**: «لا يجوز للناشر إعادة نشر المصنف إلا بعد الحصول على موافقة المؤلف وبالقدر المتفق عليه، وفي حالة مخالفة الناشر ذلك يعاقب بالعقوبة المنصوص عليها في المادة (39) من هذا القانون».

- **المادة (41)**: «لا يجوز لغير المحلات أو الأشخاص المرخص لهم بالدولة نشر أي مصنف من المصنفات أو نسخه أو طبعه، ويعاقب من يخالف ذلك بالحبس مدة لا تزيد على ستة أشهر وبالغرامة التي لا تزيد على (10000) عشرة آلاف درهم، أو بإحدى هاتين العقوبتين».

- **المادة (42)**: «لا يجوز لأي من المحلات التي تتولى توزيع أو بيع أو نسخ نماذج المصنفات أن تقوم بعملية البيع أو النسخ إلا بموافقة كتابية من المؤلف مالك المصنف أو من يخوله، ويعاقب بالحبس وبالغرامة التي لا تقل عن (50000) خمسين ألف درهم، أو بإحدى هاتين العقوبتين، صاحب المحل الذي يخالف ذلك».

ب. العقوبة التكميلية

حدد المشرع الإماراتي العقوبة التكميلية من خلال المادة (43) التي نصت أنه «في جميع الأحوال المبينة في هذا الباب يتعين الحكم بمصادرة نسخ المصنفات موضوع الجريمة، كما يجوز للمحكمة أن تحكم بإغلاق المحل».

ويلاحظ أن المشرع حصر العقوبة التكميلية في عقوبتين؛ هما:

- عقوبة المصادرة: وهي عقوبة وجوبية يتعين على القاضي أن يحكم فيها.

- عقوبة إغلاق المحل: وهي عقوبة جوازية متروكة لمحكمة الموضوع.

3. تحديد صفة مأموري الضبط القضائي الذين يحق لهم مباشرة هذه الجرائم

حدد المشرع في الفقرة الأولى من المادة (46) الجهات التي تحدد الموظفين الذين يكون لهم صفة مأموري الضبط القضائي؛ وهذه الجهات تمثل بـ:

- وزير العدل.
- وزير الإعلام والثقافة.
- السلطة المختصة في الإمارة التي تمثل جهة استشارية.

كما ذكر في الفقرة الثانية من المادة نفسها أن لمأموري الضبط القضائي، في أثناء تأدية مهماتهم، الاستعانة برجال الأمن والشرطة.

4. قانون التوقيع الإلكتروني

أصدرت دولة الإمارات العربية المتحدة عام 2002، فى إطار حرصها على تغطية الفجوة التشريعية فى مجال الاتصالات – وهو الأمر الذي يفتقده معظم الدول العربية– قانون التوقيع الإلكتروني والتجارة، وقد نص هذا القانون منع مزودي خدمات الإنترنت من كشف أي معلومات يحصلون عليها في أثناء تزويد الخدمة.[89]

الحماية القانونية في مملكة البحرين

1. الحماية الدستورية

تضمن الدستور البحريني الصادر سنة 1973 نص حرية المراسلة البريدية والبرقية والهاتفية؛ وذلك من خلال المادة (26) التي نصت أن «حرية المراسلة البريدية والبرقية والهاتفية مصونة، وسريتها مكفولة، فلا يجوز مراقبة المراسلات أو إفشاء سريتها، إلا في الضرورات التي يبينها القانون، ووفقاً للإجراءات والضمانات المنصوص عليها فيه».

2. الحماية القانونية عن طريق قانون حقوق المؤلف

صدر مرسوم قانون حقوق المؤلف برقم (10) لسنة 1993، وقد ورد ضمن هذا القانون حماية برامج الحاسب الآلي، من خلال المادة الثانية التي نصت أن «يحمي هذا القانون مؤلفي المصنفات المبتكرة الأدبية والعلمية، والفنية، والثقافية بصفة عامة، مهما كانت قيمة تلك المصنفات، أو نوعها، أو طريقة التعبير المستعملة فيها أو الغرض من تأليفها».

ثم ورد في الفقرة الأولى من المادة نفسها ضرورة أن تشمل الحماية المذكورة سابقاً مؤلفي المصنفات وفق ما يأتي: ومن ضمن هذه المصنفات ما ورد في الفقرة (ي) «برامج الحاسب الآلي المبتكرة شخصياً، بما في ذلك قاعدة البيانات. ويقصد بالبرامج المذكورة، مجموع العبارات والتعليمات المعبر عنها بأي لغة، أو رمز، أو إشارة، والمعدة للاستعمال في الحاسب الآلي، بطريق مباشرة أو غير مباشرة؛ بهدف التوصل إلى نتائج محددة».

العقوبات

1. العقوبة الأصلية

ورد ضمن المادة (37) **نص أن**: يعاقب بالحبس مدة لا تزيد على سنة، وبغرامة لا تتجاوز ألف دينار، أو بإحدى هاتين العقوبتين:

أ. كل من اعتدى على حقوق المؤلفين المنصوصة في المادتين الخامسة والسادسة من هذا القانون.

ب. كل من أدخل إلى البلاد بقصد البيع - أو باع أو تداول بقصد المتاجرة- أو روج للجمهور بأي طريقة كانت، مصنفاً مقلداً أو مزوراً.

جـ. كل من كشف -أو سهل كشف- برامج الحاسب الآلي قبل نشرها.

2. العقوبة التكميلية

حدد المشرع البحريني العقوبة التكميلية من خلال المادة (38) التي نصت أنه «يجوز للمحكمة -فضلاً عن الحكم بالعقوبة المنصوص عليها في المادة السابقة- أن تأمر بمصادرة جميع المصنفات المقلدة، والأدوات المضبوطة في الدعوى، التي استعملت في ارتكاب الجريمة، وبإتلافها».

ويلاحظ أن العقوبة التكميلية جوازية، متروك أمرها لمحكمة الموضوع.

وفي حالة العود إلى ارتكاب إحدى الجرائم المنصوصة في هذه المادة خلال ثلاث سنوات من تاريخ الحكم بالعقوبة، يجوز للمحكمة أن تقضي بالحد الأقصى للعقوبة.

الحماية القانونية في دولة قطر

1. الحماية الدستورية

نص الدستور القطري لعام 2003 حرمة خصوصية الإنسان من خلال المادة (37) التي نصت أن «لخصوصية الإنسان حرمتها، فلا يجوز تعرض أي شخص، لأي تدخل في خصوصياته أو شؤون أسرته أو مسكنه أو مراسلاته، أو أي تدخلات تمس شرفه أو سمعته، إلا وفقاً لأحكام القانون، وبالكيفية المنصوص فيه».

2. الحماية القانونية عن طريق حماية المصنفات الفكرية وحقوق المؤلف

صدر هذا القانون برقم (25) لسنة 1995؛ بشأن حماية المصنفات الفكرية وحقوق المؤلف، وقد تضمن نص حماية برامج الحاسب الآلي بوصفها من المصنفات؛ وذلك من خلال المادة (2) التي نصت أن «يتمتع بالحماية المقررة في هذا القانون، مؤلفو المصنفات المبتكرة في الآداب والفنون والعلوم، أياً كانت قيمة هذه المصنفات أو نوعيتها، أو الغرض من تأليفها، أو طريقة التعبير عنها».

كما نص في المادة (3) أن «تشمل الحماية بوجه عام، المصنفات التي يكون مظهر التعبير عنها الكتابة أو الصوت أو الرسم أو التصوير أو الحركة، وبوجه خاص ما يأتي: وقد ذُكِر في الفقرة العاشرة (برامج الحاسب الآلي وتطبيقاته، ونظم التشغيل المستوردة والمطورة محلياً)».

العقوبات

1. العقوبات الأصلية

1. المادة (42): مع عدم الإخلال بأي عقوبة أشد ينصها قانون آخر، يعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد على سنة، وبالغرامة التي لا تقل عن ثلاثين ألف ريال ولا تزيد على مئة ألف ريال، أو بإحدى هاتين العقوبتين، كل من قام بنشر مصنف غير مملوك له، من دون الحصول على إذن كتابي موثق، من مؤلف المصنف أو ورثته أو من يمثله.

ويعاقب بالعقوبة ذاتها كل من يدعي، على خلاف الحقيقة ملكيته مصنفاً غير مملوك له.

2. المادة (43): مع عدم الإخلال بأي عقوبة أشد ينصها قانون آخر، يعاقب بالحبس مدة لا تزيد على سنة، وبالغرامة التي لا تقل عن ثلاثين ألف ريال ولا تزيد على خمسين ألف ريال، أو بإحدى هاتين العقوبتين، كل ناشر قام عند نشر مصنف، بالتعديل في حقيقته أو طبيعته أو موضوعه أو عنوانه، مخالفاً بذلك تعليمات مؤلف المصنف ورغبته.

ويعاقب بالعقوبة ذاتها كل ناشر قام بإعادة نشر المصنف من دون الحصول على موافقة كتابية من المؤلف، أو بمخالفة تعليماته.

3. المادة (44): لا يجوز لغير المحال أو الأشخاص المرخص لهم في الدولة نشر أي مصنف من المصنفات أو طبعه.

ويعاقب كل من يخالف أحكام الفقرة السابقة بالحبس مدة لا تزيد على ستة أشهر، وبالغرامة التي لا تزيد على عشرة آلاف ريال، أو بإحدى هاتين العقوبتين.

4. المادة (45): لا يجوز لأي من المحال التي تتولى توزيع نماذج المصنفات أو بيعها أو نسخها، أن تقوم بعملية البيع أو النسخ إلا بموافقة كتابية من المؤلف مالك المصنف، أو من يمثله.

ويعاقب صاحب المحل الذي يخالف أحكام الفقرة السابقة، بالحبس مدة لا تزيد على سنة، وبالغرامة التي لا تقل عن ثلاثين ألف ريال ولا تزيد على خمسين ألف ريال، أو بإحدى هاتين العقوبتين.

2. العقوبة التكميلية

في جميع الأحوال المبينة في هذا الباب، يتعين الحكم بمصادرة نسخ المصنفات التي هي موضوع الجريمة، كما يجوز الحكم بإغلاق المحل. ويتضح أن المصادرة وجوبية وإغلاق المحل جوازي.

الحماية القانونية في دولة الكويت

1. الحماية الدستورية

نص الدستور الكويتي الصادر عام 1962، من خلال المادة (39) أن «حرية المراسلة البريدية والبرقية والهاتفية مصونة، وسريتها مكفولة؛ فلا يجوز مراقبة الرسائل أو إفشاء سريتها إلا في الأحوال المبينة في القانون، وبالإجراءات المنصوصة فيه».

2. الحماية القانونية عن طريق قانون حقوق الملكية الفكرية

صدر القانون بالمرسوم رقم 5 لسنة 1999، وقد تضمن حماية مصنفات الحاسب الآلي من البرامج وقواعد البيانات، من خلال المادة الأولى التي نصت أن «يتمتع بحماية هذا القانون مؤلفو المصنفات المبتكرة، في الآداب والفنون والعلوم، أياً كانت قيمة هذه المصنفات أو أنواعها أو الغرض من تأليفها أو طريقة التعبير عنها.

ويعد مؤلفاً الشخص الذي يبتكر المصنف أو ينسب إليه عند نشره، سواء أكان ذلك بذكر اسمه على المصنف أم كان بأي طريقة أخرى، إلا إذا قام الدليل على خلاف ذلك».

ونصت المادة الثانية أن تشمل الحماية بصفة خاصة المصنفات الآتية:

وقد أورد المشرع الكويتي في الفقرة (ك) من المادة نفسها «مصنفات الحاسب الآلي من برامج وقواعد بيانات وما يماثلها».

العقوبات

1. العقوبات الأصلية

نصت المادة (42) أن: يعاقب بالحبس مدة لا تزيد على سنة واحدة وبغرامة لا تزيد على خمسمئة دينار، أو بإحدى هاتين العقوبتين.

أ. كل من اعتدى على حقوق المؤلف المنصوصة في المواد 4، 5، 6، من الفقرة الأولى، و12 من هذا القانون.

ب. كل من باع مصنفاً مقلداً، أو عرضه للبيع أو للتداول، أو أذاعه على الجمهور، بأي طريقة كانت، أو أدخله إلى البلاد أو أخرجه منها.

جـ. كل من كشف –أو سهل كشف– برامج الحاسب الآلي قبل نشرها.

د. كل من أزال –أو ساعد في إزالة– حماية تنظم اطلاع الجمهور على المصنف أو الأداء أو البث أو التسجيل، أو تقيده.

2. العقوبات التكميلية

يجوز للمحكمة أن تقضي مصادرة جميع الأدوات المخصصة للنشر غير المشروع، إذا كانت لا تصلح إلا لهذا النشر، وكذلك مصادرة جميع النسخ.

ويلاحظ أن العقوبة التكميلية عقوبة جوازية متروكة لقاضي الموضوع.

3. العقوبة التبعية

يجوز للمحكمة أن تأمر بنشر الحكم في جريدة واحدة أو أكثر، على نفقة المحكوم عليه.

4. تشديد العقوبة

إذا سبق الحكم على المتهم بعقوبة لارتكابه إحدى الجرائم المشار إليها في هذه المادة، وثبت ارتكابه خلال خمس سنوات من تاريخ الحكم النهائي جريمة من الجرائم السابقة، جاز للمحكمة أن تقضي في هذه الجريمة عقوبة تزيد على الحد الأقصى المقرر قانوناً، شرط ألا تجاوز الزيادة نصف هذا الحد، وبغلق المنشأة التي استغلت في ارتكاب الجريمة مدة لا تزيد على ستة أشهر.

الحماية القانونية في سلطنة عُمان

1. الحماية الدستورية

نص النظام الأساسي للسلطنة الذي صدر عام 1996، في المادة (30) أن «حرية المراسلات البريدية والبرقية والمخاطبات الهاتفية وغيرها من وسائل الاتصال مصونة، وسريتها مكفولة، فلا يجوز مراقبتها أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها إلا في الحالات التي يبينها القانون وبالإجراءات المنصوص فيه».

2. الحماية القانونية عن طريق قانون حقوق المؤلف والحقوق المجاورة

صدر القانون برقم 37/ 2000 لعام 2000، وقد تم تعريف برامج الحاسب الآلي من خلال المادة الأولى التي يقصد بها: مجموع العبارات والتعليمات المعبر عنها بأي لغة أو رمز أو إشارة، والمعدة للاستعمال في الحاسب الآلي بطريق مباشر أو غير مباشر؛ بهدف التوصل إلى نتائج محددة.

كما أُورد من خلال المادة الثانية أن «يتمتع بحماية هذا القانون مؤلفو المصنفات المبتكرة الأدبية والعلمية والفنية والثقافية بصفة عامة، مهما كانت قيمة تلك المصنفات أو نوعها أو طريقة التعبير المستعملة فيها أو الغرض من تأليفها، وتشمل الحماية على الأخص مؤلفي المصنفات الآتية:

أ. الكتب وبرامج الحاسب الآلي وغيرها من المواد المكتوبة».

العقوبات

1. العقوبات الأصلية

يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تجاوز ألفي ريال عُماني، أو بإحدى هاتين العقوبتين كل من اعتدى على حق من الحقوق الأدبية أو المالية للمؤلف أو لأصحاب الحقوق المجاورة وفقاً لأحكام هذا القانون، ويعد اعتداءً بوجه خاص قيام المعتدي بعمل أو أكثر مما يأتي:

أ. البيع أو الطرح للتداول بأي صورة من الصور لمصنف محمي طبقاً لأحكام هذا القانون.

ب. التقليد في سلطنة عُمان لمصنف منشور في الخارج، أو طرحه للتداول، أو تصديره أو شحنه إلى الخارج، مع العلم بتقليده.

جـ. إتاحة الأداء أو البث الإذاعي أو التسجيل السمعي للجمهور أو وضعه في متناوله عبر شبكة اتصالات تعمل بواسطة الحاسبات؛ لغرض تجاري.

د. الإزالة أو المسح من دون وجه حق لأي حماية تقنية تنظم اطلاع الجمهور على المصنف أو الأداء أو البث أو التسجيل أو التوزيع أو الاستيراد أو تقيده؛ بغرض التوزيع أو البث أو الإتاحة للجمهور لشيء مما تقدم. ويشترط في ذلك أن يكون مرتكب الفعل عالماً أو في إمكانه أن يعلم بالاعتداء الواقع.

2. العقوبات التكميلية

أ. تقضي المحكمة بمصادرة النسخ المقلدة والأدوات المستخدمة في التقليد.

ب. يجوز للمحكمة عند الحكم بالإدانة أن تقضي بغلق المنشأة التي استغلها المقلدون.

3. تشديد العقوبة

في حالة العود تضاعف العقوبة.

ويلاحظ أن دول مجلس التعاون اهتمت جميعاً بحماية وسائل الاتصال بشكل عام، عن طريق الدساتير والنظم الأساسية، ويدخل في هذه الحماية، بطبيعة الحال، البيانات والبرامج والمواقع التي تستخدم الاتصالات.

ونصوص الدستور، وإن كانت تتضمن الحماية، فإنها نصوص عامة تترك التفصيلات لنظم أخرى مكملة لها؛ مثل: نظم الاتصال وقوانينه، ونظم مكافحة الجرائم المعلوماتية وقوانينها، التي تحدد آلية الحماية عن طريق سياسة التجريم والعقاب.

كما اهتمت الدول الخليجية بحماية برامج الحاسب الآلي وقواعد البيانات؛ بوصفها من المصنفات المحمية بقوانين حماية الملكية الفكرية وحقوق المؤلف، وهو ما درج عليه أغلب دول العالم.

2. الحماية الجنائية للمعلومات في دول مجلس التعاون

مما تقدم يتضح أن دول مجلس التعاون لدول الخليج العربية سعت إلى حماية المعلوماتية، من خلال حماية نظم الاتصال وحرمتها، وأهمية المحافظة على سريتها، وعدم إطلاع الآخرين عليها، حتى لو كانت السلطات الرسمية، ماعدا الأحوال التي حددتها القوانين والنظم، وبضوابط خاصة. وقد بدئت الحماية من خلال الدساتير التي تعد القوانين العليا في التدرج التشريعي. وتركت التفاصيل لنظم أخرى.

وبما أن الدساتير غالباً نصوص لا يمكن تطبيقها مباشرة، وللزيادة المطردة في استخدام وسائل التقنية الحديثة، والاعتماد عليها في منطقة الخليج،

وبروز ظاهرة التعدي على البرامج والبيانات والكيان المنطقي للحاسب الآلي بأفعال تعد من قبيل الجرائم، ولا يمكن تطبيق نصوص التجريم التقليدية عليها، فقد ظهرت الحاجة إلى قوانين ونظم أخرى.

كما لجأت دول مجلس التعاون إلى نظم حماية الملكية الفكرية وحقوق المؤلف وقوانينها؛ لحماية البرامج والبيانات بوصفها من المصنفات الفكرية؛ لمواجهة الفراغ التشريعي الذي لم يتم التغلب عليه من خلال النظم السابقة.

ونظراً إلى إحساس دول مجلس التعاون بخطورة الجرائم المعلوماتية وتزايدها، فقد أوصى بإصدار نظم وقوانين لمواجهتها، وهذا ما يتفق وما أُصدر في أيار/ مايو 2006 بمناسبة الاحتفال بمرور خمسة وعشرين عاماً (اليوبيل الفضي) على قيام مجلس التعاون لدول الخليج العربية في 25/ 5/ 1981؛ حيث أوصى المجلس ببعض التوصيات التي من ضمنها التعاون في مجال الاتصال. وقد أُورد من ضمن التوصيات «حث الجهات المعنية بالدول الأعضاء على الإسراع باستصدار نظم وقوانين لمكافحة الجرائم المعلوماتية والحاسب الآلي والإنترنت».

3. النظم والقوانين الجنائية التي صدرت في دول مجلس التعاون

تبرز دول مجلس التعاون في مجال مواجهة الجرائم المعلوماتية، فهي أولى الدول العربية التي أوجدت نظماً وقوانين لمواجهتها، سواء عن طريق تعديل قانون العقوبات مثل سلطنة عُمان، أو عن طريق إصدار نظم وقوانين مستقلة مثل دولة الإمارات العربية المتحدة، والمملكة العربية السعودية.

أ. الحماية الجنائية في سلطنة عُمان

يعد أول قانون عربي لمواجهة الجرائم المعلوماتية هو القانون العُماني من خلال التعديل الذي أُدخل على قانون الجزاء العُماني رقم 7 الذي صدر عام 1974، بموجب المرسوم السلطاني رقم 72/ 2001، ومن ضمن هذه التعديلات إضافة الفصل الثاني مكرر على الباب السابع تحت عنوان جرائم الحاسب الآلي، ويعد هذا القانون باكورة القوانين العربية في مجال مواجهة الجرائم المعلوماتية من خلال تعديل قانون العقوبات.

وينص القانون الخاص بجرائم الحاسب الآلي في المادة (276) مكرر أن يعاقب بالسجن مدة لا تقل عن ثلاثة أشهر، ولا تزيد على السنتين، وبغرامة من مئة ريال عُماني إلى خمسمئة ريال عُماني، أو بإحدى هاتين العقوبتين، لكل من تعمد استخدام الحاسب الآلي في ارتكاب أحد الأفعال الآتية:

1. الالتقاط غير المشروع للمعلومات أو البيانات.
2. الدخول غير المشروع على نظم الحاسب الآلي.
3. التجسس والتنصت على البيانات والمعلومات.
4. انتهاك خصوصيات "الغير" أو التعدي على حقهم في الاحتفاظ بأسرارهم وتزوير البيانات أو الوثائق المبرمجة أياً كان شكلها.
5. إتلاف البيانات والمعلومات وتغييرها ومحوها.
6. جمع المعلومات والبيانات وإعادة استخدامها.

7. تسريب المعلومات والبيانات.

8. التعدي على برامج الحاسب الآلي سواء بالتعديل أو الاصطناع.

9. نشر برامج الحاسب الآلي واستخدامها، بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية.

- مادة (276) مكرراً (1): يعاقب بالسجن مدة لا تقل عن ستة أشهر ولا تزيد على السنتين، وبغرامة لا تقل عن مئة ريال عُماني ولا تزيد على خمسمئة ريال عُماني، أو بإحدى هاتين العقوبتين، كل من استولى على البيانات التي تخص "الغير"، أو حصل عليها على نحو غير مشروع، وتكون منقولة أو مختزنة أو معالجة بواسطة نظم المعالجة المبرمجة للبيانات.

- مادة (276) مكرراً (2): تضاعف العقوبة إذا ارتكب مستخدمو الكمبيوتر الأفعال المشار إليها في المادة (276) مكرراً و(276) مكرراً (1).

- مادة (276) مكرراً (3): يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تتجاوز ألف ريال عُماني كل من:

1. قام بتقليد بطاقة من بطاقات الائتمان أو السحب أو تزويرها.

2. استعمل البطاقة المقلدة أو المزورة أو حاول استعمالها، مع العلم بذلك.

3. قبِل الدفع ببطاقة الائتمان المقلدة أو المزورة، مع العلم بذلك.

- مادة (276) مكرراً (4): يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تتجاوز خمسمئة ريال عُماني كل من:

1. استخدم البطاقة وسيلة للسحب، مع علمه بعدم وجود رصيد له.

2. استعمل البطاقة بعد انتهاء صلاحيتها أو إلغائها، وهو على علم بذلك.

3. استعمل بطاقة "الغير" من دون علمه.

ب. الحماية الجنائية في دولة الإمارات العربية المتحدة

تعد دولة الإمارات العربية المتحدة أول دولة عربية تصدر قانوناً مختصاً في مكافحة جرائم المعلومات؛ حيث أصدر صاحب السمو الشيخ خليفة بن زايد آل نهيان رئيس الدولة، القانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات.

ويتكون القانون من تسع وعشرين مادة، اشتملت على الآتي:

1. التعريفات

بدئ القانون بالمادة الأولى التي تحتوي على الكثير من التعريفات التي توضح معاني العبارات الواردة في النظام، وهو مسلك قانوني مهم خاصة عند تطبيق القانون.

2. الجرائم

حدد المشرع الإماراتي الأفعال التي يعد ارتكابها جريمة من جرائم المعلومات، كما حدد العقوبات الملائمة لها تبعاً لخطورتها وضررها المتوقع، وقد شمل القانون أغلب الجرائم المعلوماتية؛ وهي:

- التوصل بغير وجه حق إلى موقع أو نظام معلوماتي بدخول الموقع أو النظام، أو بتجاوز مدخل مصرح به.

- إلغاء بيانات أو معلومات أو حذفها أو تدميرها أو إفشاؤها أو إتلافها أو تغييرها أو إعادة نشرها.

- التعدي على البيانات الشخصية.

- تزوير مستند من مستندات الحكومة الاتحادية أو المحلية، أو الهيئات أو المؤسسات العامة الاتحادية والمحلية، معترف به قانوناً في نظام معلوماتي.

- استعمال المستند المزور، مع علم الجاني بتزويره.

- إعاقة الوصول إلى الخدمة أو مصادر البيانات أو المعلومات بأي وسيلة كانت، أو الدخول إلى الأجهزة أو البرامج أو تعطيلها، سواء عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات.

- الإدخال عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، ما من شأنه وقفها عن العمل، أو تعطيلها، أو التدمير أو المسح أو الحذف أو الإتلاف أو التعديل للبرامج أو البيانات أو المعلومات فيها.

- التعديل أو الإتلاف للفحوص الطبية، أو التشخيص الطبي، أو العلاج الطبي، أو الرعاية الطبية، أو التسهيل لـ "الغير" فعل ذلك، أو تمكينه منه، باستعمال الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات.

- التنصت أو الالتقاط أو الاعتراض عمداً، من دون وجه حق، لما هو مرسل عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات.

- استعمال الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات في تهديد أو ابتزاز لشخص آخر؛ لحمله على القيام بالفعل أو الامتناع عنه.

- التهديد بارتكاب جناية، أو بإسناد أمور خادشة للشرف، أو الاعتبار.

- استيلاء الشخص لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند؛ وذلك بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة، متى كان ذلك من شأنه خداع المجني عليه.

- الوصول من دون وجه حق، إلى أرقام أو بيانات لبطاقة ائتمانية أو غيرها من البطاقات الإلكترونية.

- استيلاء الشخص لنفسه أو لغيره على مال "الغير".

- الإنتاج أو الإعداد أو التهيئة أو الإرسال أو التخزين؛ بقصد الاستغلال أو التوزيع أو العرض على "الغير" عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات لما من شأنه المساس بالآداب العامة، أو إدارة مكان لذلك. وتشدد العقوبة في حال توجيه الفعل للحدث.

- من حرض ذكراً أو أنثى، أو أغواه لارتكاب الدعارة أو الفجور أو ساعده على ذلك، باستخدام الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات. وتشدد العقوبة في حال توجيه الفعل للحدث.

- الدخول من دون وجه حق إلى موقع في الشبكة المعلوماتية؛ لتغيير تصميمات هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه.

- الإساءة إلى أحد المقدسات، أو إحدى الشعائر الإسلامية.

- الإساءة إلى أحد المقدسات، أو إحدى الشعائر المقررة في الأديان الأخرى، متى كانت هذه المقدسات والشعائر مصونة؛ وفقاً لأحكام الشريعة الإسلامية.

- سب أحد الأديان السماوية المعترف بها.

- تزيين المعاصي، أو الحض عليها، أو الترويج لها.

- مناهضة الدين الإسلامي، أو جرح الأسس والمبادئ التي يقوم عليها، أو المناهضة أو الجرح لما علم من الدين الإسلامي بالضرورة، أو النيل من الدين الإسلامي، أو التبشير بغيره، أو الدعوة إلى مذهب، أو فكرة تنطوي على شيء مما تقدم، أو فُضِّل ذلك أو رُوِّج له.

- الاعتداء على أي مبدأ من المبادئ أو القيم الأسرية أو نشر أخبار أو صور تتصل بحرمة الحياة الخاصة أو العائلية للأفراد ولو كانت صحيحة، عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات.

- الاتجار بالأشخاص أو تسهيل التعامل فيه.

- ترويج المخدرات أو المؤثرات العقلية وما في حكمهما، أو تسهيل التعامل فيهما؛ وذلك في غير الأحوال المصرح بها قانوناً.

- غسل الأموال.

- التسهيل والترويج لبرامج وأفكار، من شأنها الإخلال بالنظام العام والآداب العامة.

- إنشاء موقع أو نشر معلومات على الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، لجماعة إرهابية تحت مسميات تمويهية؛ لتسهيل الاتصالات بقياداتها، أو أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرة، أو أي أدوات تستخدم في الأعمال الإرهابية.

- الدخول بغير وجه حق إلى موقع أو نظام مباشرة، أو عن طريق الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات؛ بقصد الحصول على بيانات أو معلومات حكومية سرية؛ إما بطبيعتها وإما بمقتضى تعليمات صادرة بذلك.

- تشدد العقوبة إذا ترتب على الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها. ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت المالية الأخرى والتجارية والاقتصادية.

3. العقوبات الأصلية

حصر المشرع الإماراتي العقوبات الأصلية في ثلاثة أنواع؛ هي: السجن المؤقت، والحبس، والغرامة.

ومما يلفت الانتباه -في رأيي- أن المشرع الإماراتي ترك للقاضي سلطة تقديرية كبيرة بعدم تحديد العقوبة في بعض المواد التي نص عقوبتها بالنص الآتي: «يعاقب بالحبس وبالغرامة، أو بإحدى هاتين العقوبتين».

كما نص في بعض المواد (السجن المؤقت)، وجعل السجن أو الغرامة أو بهما معاً؛ تشديداً في حال ارتكاب الفعل في حالات خاصة.

وفي حالات أخرى يذكر العقوبة بالحبس وبالغرامة من دون تحديد لهما، ثم يشدد العقوبة في حالة خاصة، ويحدد مقدارها وفق ما ورد في المادة الثانية عشرة.

4. العقوبات التكميلية

- المصادرة

مع عدم الإخلال بحقوق "الغير" الحسن النية؛ يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي جريمة من الجرائم المنصوصة في هذا القانون، أو الأموال المتحصلة منها.

- إغلاق المحل

يحكم بإغلاق المحل، أو الموقع الذي يرتكب فيه أي من هذه الجرائم؛ إذا كانت الجريمة قد ارتكبت بعلم مالكه؛ وذلك إغلاقاً كلياً أو المدة التي تقدرها المحكمة.

- الإبعاد

- فضلاً عن العقوبات المنصوصة في هذا القانون، تقضي المحكمة بإبعاد الأجنبي الذي يحكم عليه بالحبس وفقاً لأحكام هذا القانون.

5. الإسهام الجنائي

كل من حرض "الغير" أو ساعده أو اتفق وإياه، على ارتكاب جريمة من الجرائم المنصوصة في هذا القانون، ووقعت الجريمة بناء على هذا التحريض أو المساعدة أو الاتفاق، يعاقب بالعقوبة ذاتها المقررة لها.

6. مأمورو الضبط القضائي

تكون للموظفين الذين يصدر قرار من وزير العدل والشؤون الإسلامية والأوقاف، بتحديدهم بصفة مأموري الضبط القضائي، صلاحيات ضبط الجرائم والمخالفات التي تقع بالمخالفة لأحكام هذا القانون، وعلى السلطات المحلية بالإمارات تقديم التسهيلات اللازمة لهؤلاء الموظفين لتمكينهم من القيام بعملهم.

ج. الحماية الجنائية في المملكة العربية السعودية

تعد المملكة العربية السعودية الدولة العربية الثالثة التي أصدرت نظاماً لمكافحة الجرائم المعلوماتية بموجب المرسوم الملكي رقم(17) لعام 1428هـ، ويتكون من ست عشرة مادة ولا يختلف كثيراً عن القانون الإماراتي من حيث التجريم ونوعية الجرائم، إلا أن المنظم السعودي حدد العقوبة لكل فعل من خلال بداية كل مادة بعقوبة معينة، ثم إدراج عدد من الجرائم تحت كل مادة.

وقد حدد النظام السعودي أغلب الجرائم المعلوماتية، التي شملت الأفعال التي تشكل خطراً على المعلومات، إضافة إلى الأحكام الخاصة بالإسهام الجنائي، وتشديد العقوبة، والشروع فيها، والإعفاء من العقاب، والعقوبة التكميلية.

ومن السمات العامة للنظام السعودي والقانون الإماراتي ما يأتي:

1. وضوح الألفاظ والمعاني عن طريق إفراد مادة، تعنى بالمصطلحات الواردة في النظام أو القانون وإيضاح معانيها حتى لا تثير بعض الإشكالات عند التطبيق.
2. تطبيق مبدأ الشرعية الجنائية من خلال الدقة والوضوح في نصوص التجريم؛ وذلك بتحديد الصور الجرمية التي يشملها النص والتي تغطي أغلب الجرائم المعلوماتية وتحديد العقوبات المناسبة لها.[90]
3. التدرج في العقوبة تبعاً لجسامة الجريمة ووضوح أركانها.
4. إيضاح أهداف النظام السعودي من خلال إفراد مادة خاصة بذلك.
5. بيان الظروف المشددة للعقوبة.
6. تحديد صور الاشتراك في الجريمة.
7. نص عقوبة الشروع في النظام السعودي.
8. تحديد حالات الإعفاء من العقاب في النظام السعودي.
9. التكامل والأحكام الواردة في النظم ذات العلاقة بحقوق الملكية الفكرية والاتفاقات الدولية ذات الصلة بذلك.

10. نص العقوبة التكميلية، مع الإشارة إلى حسن النية.

11. تحديد الجهات ذات العلاقة بتطبيق أحكام النظام.

12. التقيد بسريان النصوص الجنائية من حيث الزمان.

13. وضوح الاهتمام بما يتعلق بالشريعة الإسلامية وتجريم المساس بها، ومناهضتها، أو الإساءة إليها.

ويعد صدور النظام السعودي والقانون الإماراتي، من الأمور المهمة التي ستغطي الفراغ التشريعي الذي يعانيه أغلب دول العالم، وخاصة بتزايد الاعتماد على وسائل التقنية الحديثة على المستويين: الرسمي والشخصي في دول مجلس التعاون لدول الخليج العربية.

ومهما كان في النظام السعودي والقانون الإماراتي من قصور فإن المعالجة النظامية والقانونية كفيلة بالتعديل، وخاصة بعد التجربة والتطبيق، وظهور أوجه القوة والضعف ومكامن الخلل.

وإن إصدار اللوائح التنفيذية للنظام والقانون الآنفي الذكر -في رأيي- قد يجيب عن بعض التساؤلات، ويكشف الغموض والعمومية التي تظهر في بعض المواد.

الخاتمة

بعد أن تم التطرق إلى الجرائم المعلوماتية وإيضاح مفهومها وحجمها ودوافعها وخصائصها وأقسامها، وإيضاح الاتجاهات المختلفة لتحديد

الطبيعة القانونية للمعلومات، وفاعلية نصوص التجريم التقليدية في مواجهة الجرائم المعلوماتية، اتضح من خلال الدراسة أن تلك النصوص تواجه بعض العقبات تتمثل في أنها وضعت لمواجهة الجرائم ذات الطبيعة المادية، على حين أن الجرائم المعلوماتية ذات جانب معنوي تتميز به من الجرائم الأخرى.

وإدراكاً لقصور القوانين الجنائية بما تتضمنه من نصوص التجريم التقليدية، وخضوعها للقواعد التي تحكم نظام العقاب الجزائي -وهي المتمثلة في مبدأ الشرعية الجنائية وحظر القياس في المواد الجنائية- كان لابد من المواجهة التشريعية التي تتناسب والتطور الملحوظ في جرائم المعلوماتية، من خلال قواعد قانونية غير تقليدية لهذا الإجرام غير التقليدي.

ويتم ذلك من خلال محورين: الأول داخلي بحيث تتواءم فيه تشريعات الدول وهذا النمط من الإجرام، والثاني دولي عن طريق عقد الاتفاقيات الدولية؛ حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية، وغياب الاتفاقيات الدولية التي تعالج سبل مواجهة هذه الجرائم.

وبناء على ذلك عُقدت الاتفاقيات الدولية، وتم إصدار قوانين لمواجهة الجرائم المعلوماتية في كثير من الدول، إلا أنه مايزال هناك ضعف في التعاون الدولي والتنسيق بين الدول على المستوى الإقليمي، وخاصة في الدول العربية.

وتعد دول مجلس التعاون لدول الخليج العربية أولى الدول العربية التي واجهت الجرائم المعلوماتية، من خلال التعديل الذي أُجري على قانون العقوبات في سلطنة عُمان، وإصدار نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية لعام 1428هـ، والقانون الإماراتي للغرض نفسه عام 2006.

النتائج والتوصيات

من خلال ما تم تناوله في هذه الدراسة توصل الباحث إلى عدد من النتائج والتوصيات على النحو الآتي:

أولاً: النتائج

1. عدم الاتفاق على مفهوم موحد للجرائم المعلوماتية.
2. اختلاف تقسيمات الجرائم المعلوماتية تبعاً للنظرة القانونية إليها.
3. عدم الاتفاق على تحديد الطبيعة القانونية للمعلومة.
4. اختلاف سمات الجرائم المعلوماتية عن الجرائم التقليدية.
5. عدم كفاية النصوص القانونية المعنية بالجرائم التقليدية لمواجهة الجرائم المعلوماتية.
6. أخذ معظم دول العالم بنظم حماية الملكية الفكرية وحقوق المؤلف؛ لحماية المعلومات بوصفها من المصنفات، ولسد الفراغ التشريعي الذي تعانيه.

7. الحاجة إلى إصدار قوانين ونظم؛ لمواجهة الجرائم المعلوماتية.

8. ضعف التعاون الدولي في مجال مكافحة الجرائم المعلوماتية.

9. اختلاف سبل الحماية القانونية في الدول التي أصدرت بعض النظم في هذا الخصوص.

10. تميز الدول الأوربية في مواجهة الجرائم المعلوماتية.

11. ضعف المواجهة القانونية للجرائم المعلوماتية في الدول العربية بشكل عام.

12. أسبقية دول مجلس التعاون، إقليمياً، في مكافحة الجرائم المعلوماتية، بقوانين ونظم خاصة.

ثانياً: التوصيات

1. زيادة التعاون الدولي؛ لمواجهة الجرائم المعلوماتية عن طريق الاتفاقيات والمعاهدات الدولية.

2. ضرورة عقد المؤتمرات والندوات الدولية؛ للوصول إلى تحديد مفهوم عام للجرائم المعلوماتية.

3. زيادة مستوى التعاون العربي لمواجهة هذه الجرائم.

4. إصدار القوانين والنظم الخاصة لمواجهة الجرائم المعلوماتية على مستوى الدول.

5. أهمية التعاون الخليجي لمواجهة هذه الجرائم عن طريق المعاهدات والنظم المشتركة.

الهوامش

1. انظر: أحمد خليفة الملط، **الجرائم المعلوماتية** (الإسكندرية: دار الفكر الجامعي، 2005)، ص89، 90.
2. محمد عبدالله سلامة، **جرائم الكمبيوتر والإنترنت** (الإسكندرية: منشأة المعارف، 2006)، ص74.
3. أحمد خليفة الملط، مرجع سابق، ص96.
4. أسامة أحمد المناعسة وآخرون، **جرائم الحاسب الآلي والإنترنت** (عمان: دار وائل، 2001)، ص77، 78.
5. محمد سامي الشوا، **ثورة المعلومات وانعكاساتها على قانون العقوبات** (القاهرة: دار النهضة العربية، 1994)، ص6.
6. نائلة عادل قورة، **جرائم الحاسب الآلي الاقتصادية** (بيروت: منشورات الحلبي، 2005)، ص67.
7. يونس عرب، «جرائم الكمبيوتر والإنترنت»، ورقة عمل مقدمة إلى مؤتمر الأمن العربي، المركز العربي للدراسات والبحوث الجنائية، أبوظبي، 2002، ص1.
8. عبدالفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت** (الإسكندرية: دار الفكر الجامعي، 2006)، ص68، 67.
9. الإيكو (E.C.U) هو وحدة النقد الأوربية.
10. أحمد خليفة الملط، مرجع سابق، ص111.
11. يقصد بالقرصنة الفكرية: سرقة برامج الحاسب الآلي المطورة، ونسخها أو فك رموزها، ثم ترويجها من دون إذن أو حق. وهذا يلحق خسائر كبيرة بالشركات وأصحاب البرامج الأصلية أو واضعيها وأصحاب الحقوق الفكرية عليها.
12. محمود عبدالرحيم الديب، **الحماية القانونية للملكية الفكرية في مجال الحاسب الآلي والإنترنت** (الإسكندرية: دار الجامعة الجديدة، 2005)، ص75، 74.

13. محمود أحمد عبابنة، **جرائم الحاسوب وأبعادها الدولية** (عمان: دار الثقافة، 2005)، ص24.
14. أحمد خليفة الملط، مرجع سابق، ص100.
15. المرجع السابق، ص101، 102.
16. انظر: نظام مكافحة جرائم المعلوماتية السعودي، الفقرة الثانية من المادة الثالثة.
17. محمود أحمد عبابنة، مرجع سابق، ص27، 28.
18. محمد أمين الشوابكة، **جرائم الحاسوب والإنترنت** (عمان: مكتبة دار الثقافة، 2007)، ص29.
19. عمر محمد أبوبكر بن يونس، **الجرائم الناشئة عن استخدام الإنترنت** (القاهرة: دار النهضة العربية، 2004)، ص 336.
20. محمد أمين الشوابكة، مرجع سابق، ص237، 238.
21. انظر: محمد عبد المحسن المقاطع، **حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي** (الكويت: ذات السلاسل، 1992)، ص 96- 103.
22. جميل عبدالباقي الصغير، **الإنترنت والقانون الجنائي** (القاهرة: دار النهضة العربية، 2002)، ص33.
23. حسام شوقي، **حماية وأمن المعلومات على الإنترنت** (القاهرة: دار الكتب العلمية، 2003) ص85.
24. عبدالفتاح مراد، **شرح جرائم الكمبيوتر والإنترنت** (الإسكندرية، د.ت)، ص55.
25. المرجع السابق، ص 56.
26. جميل عبدالباقي الصغير، مرجع سابق، ص 42.
27. عمر محمد بن يونس، مرجع سابق، ص685، 686.
28. محمد سامي الشوا، مرجع سابق، ص178، 179.

29. السيد عتيق، **جرائم الإنترنت** (القاهرة: دار النهضة العربية، 2002)، ص88.
30. محمد سامي الشوا، مرجع سابق، ص 183.
31. المرجع السابق، ص 183.
32. نائلة عادل قورة ، مرجع سابق، ص120.
33. المرجع السابق، ص 120.
34. محمد علي العريان، **الجرائم المعلوماتية** (الإسكندرية: دار الجامعة الجديدة للنشر، 2004)، ص51.
35. السيد عتيق، مرجع سابق، ص89، 90.
36. محمد سامي الشوا، مرجع سابق، ص186.
37. يقصد بالتكييف القانوني للوقائع، إجراء عملية مطابقة تامة بين النموذج الواقعي للفعل، مع النموذج القانوني الوارد في النص الجنائي، ونتيجة التكييف: أنه إذا تطابق النموذج الواقعي والنموذج القانوني، كان الفعل جريمة تستند إلى النص القانوني المتضمن لها ذاته. انظر: أسامة أحمد المناعسة وآخرين، مرجع سابق، ص36.
38. جميل عبدالباقي الصغير، **القانون الجنائي والتكنولوجيا الحديثة** (القاهرة: دار النهضة العربية، 1992)، ص18، 19.
39. كير أورين، «نطاق الجريمة الافتراضية»، ترجمة: عمر محمد يونس، **مجلة القانون**، العدد 78 (جامعة نيويورك: تشرين الثاني/ نوفمبر 2003)، ص30، 31.
40. محمد علي العريان، مرجع سابق، ص103.
41. جميل عبدالباقي الصغير، مرجع سابق، ص22.
42. يونس عرب، مرجع سابق، ص2.
43. محمد علي العريان، مرجع سابق، ص 18.
44. عبدالفتاح مراد، مرجع سابق، ص33.

45. محمود محمود مصطفى، **شرح قانون العقوبات: القسم العام**، ط3 (القاهرة: دار النيل للطباعة، 1955)، ص 26، 27.

46. محمود نجيب حسني، **شرح قانون العقوبات: القسم العام**، ط4 (القاهرة: دار النهضة العربية، 1997)، ص 77. وانظر: «النظام الأساسي للحكم في المملكة العربية السعودية» المادة 38، وانظر: الدستور الإماراتي، المادة رقم 27.

47. عمر محمد بن يونس، مرجع سابق، ص155.

48. مدحت رمضان، **جرائم الاعتداء على الأشخاص والإنترنت** (القاهرة: دار النهضة العربية، 2000)، ص30.

49. انظر: محمد علي العريان ، مرجع سابق، ص 103.

50. جميل عبدالباقي الصغير، مرجع سابق، ص19.

51. عمر محمد بن يونس، مرجع سابق، ص 189.

52. السيد عتيق، مرجع سابق، ص 91، 92.

53. يونس عرب، «صور الجرائم الإلكترونية واتجاهاتها وتبويبها»، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية (مسقط، 2006)، ص7.

54. محمود صالح العادلي، «الجرائم المعلوماتية ماهيتها وصورها»، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية (مسقط، 2006)، ص3.

55. داود حسن طاهر، جرائم نظم المعلومات (الرياض: أكاديمية نايف العربية، 2000)،ص210.

56. محمد عمر بن يونس، مرجع سابق، ص168، 169.

57. انظر: وليد الزيدي، **القرصنة على الإنترنت والحاسوب** (عمان: دار أسامة، 2003) ص161، 162.

58. أحمد خليفة الملط، مرجع سابق، ص 670.

59. محمود أحمد عبابنة، مرجع سابق، ص 117.

60. أحمد خليفة الملط، مرجع سابق، ص 673.

61. يونس عرب، مرجع سابق، ص 2.

62. نائلة عادل قورة، مرجع سابق، ص 55.

63. وليد الزيدي، مرجع سابق، ص 149، 150.

64. محمود أحمد عبابنة، مرجع سابق، ص 158.

65. هلالي عبدالله أحمد، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 تشرين الثاني/ نوفمبر 2001** (القاهرة: دار النهضة العربية، 2003)، ص32.

66. انظر: نائلة عادل قورة، مرجع سابق، ص 305، 306.

67. المرجع السابق، ص 311.

68. يونس عرب، «قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وسلطنة عُمان»، ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية، (مسقط: 2006)، ص 2.

69. نائلة عادل قورة، مرجع سابق، ص 406 – 409.

70. محمود أحمد عبابنة، مرجع سابق، ص143.

71. http://usinfo.state.gov/ar/Archive/2006/Aug/1069758.htm1

72. أحمد خليفة الملط، مرجع سابق ص، 164.

73. المرجع السابق، ص 169– 170.

74. عماد محمد سلامة، **الحماية القانونية لبرامج الحاسب الآلي** (عمان: دار وائل، 2005)، ص 104.

75. محمود أحمد عبابنة، مرجع سابق، ص 149.

76. أحمد خليفة الملط، مرجع سابق 158.

77. عماد محمد سلامة، مرجع سابق، ص 104.
78. أحمد خليفة الملط، مرجع سابق، ص 145، 146.
79. عماد محمد سلامة، مرجع سابق، ص 108.
80. أحمد خليفة الملط، مرجع سابق، ص 162- 164.
81. يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية، مرجع سابق، ص 5، 4.
82. محمود أحمد عبابنة، مرجع سابق، 170، 171.
83. http://www.aticm.org.eg
84. يونس عرب، مرجع سابق، ص 27.
85. صدر النظام الأساسي للحكم في المملكة العربية السعودية بموجب بالأمر الملكي رقم (أ/ 90) في تاريخ 27/ 8/ 1412هـ.
86. جريدة أم القرى، العدد رقم 3849 وتاريخ 1422/4/8هـ.
87. جريدة أم القرى، العدد رقم 4042 وتاريخ 1426/3/20هـ.
88. جريدة أم القرى، العدد رقم 3959 وتاريخ 1424/7/23هـ.
89. http://www.openarab.net/reports/net2006/uae.shtml
90. انظر: النظام الأساسي للحكم في المملكة العربية السعودية المادة 38، والدستور الإماراتي المادة رقم 27.

نبذة عن المحاضر

الدكتور ناصر بن محمد البقمي، حاصل على درجتي الدكتوراه والماجستير في جامعة نايف العربية للعلوم الأمنية.

ويعمل عضو هيئة تدريس في قسم العلوم الشرعية والقانونية في كلية الملك فهد الأمنية بالمملكة العربية السعودية منذ عام 1983؛ حيث يقوم بتدريس مادتي الأنظمة الجنائية وحقوق الإنسان، إضافة إلى بعض المقررات ذات العلاقة بالقانون الجنائي.

قدم عدداً من البحوث في مجالي القانون الجنائي؛ منها: «الطاعة في الوظيفة كسبب من أسباب الإباحة»، و«غسل الأموال: التجريم والمكافحة»، و«فاعلية التشريعات العقابية في مكافحة الجرائم المعلوماتية».

من مؤلفاته: **كتاب الاتصالات**، وكتاب **مواجهة الجرائم المعلوماتية**.

صدر من سلسلة
محاضرات الإمارات

1. بريطانيا والشرق الأوسط: نحو القرن الحادي والعشرين

مالكولم ريفكند

2. حركات الإسلام السياسي والمستقبل

د. رضوان السيد

3. اتفاقية الجات وآثارها على دول الخليج العربية

محمد سليم

4. إدارة الأزمات

د. محمد رشاد الحملاوي

5. السياسة الأمريكية في منطقة الخليج العربي

لينكولن بلومفيلد

6. المشكلة السكانية والسلم الدولي

د. عدنان السيد حسين

7. مسيرة السلام وطموحات إسرائيل في الخليج

د. محمد مصلح

8. التصور السياسي لدولة الحركات الإسلامية

خليل علي حيدر

9. الإعلام وحرب الخليج: رواية شاهد عيان

بيتر آرنيت

10. الشورى بين النص والتجربة التاريخية

د. رضوان السيد

11. مشكلات الأمن في الخليج العربي
منذ الانسحاب البريطاني إلى حرب الخليج الثانية

د. جمال زكريا قاسم

12. التجربة الديمقراطية في الأردن: واقعها ومستقبلها

هاني الحوراني

13. التعليم في القرن الحادي والعشرين

د. جيرزي فياتر

14. تأثير تكنولوجيا الفضاء والكومبيوتر على أجهزة الإعلام العربية

محمد عارف

15. التعليم ومشاركة الآباء بين علم النفس والسياسة

دانييل سافران

16. أمن الخليج وانعكاساته على دول مجلس التعاون لدول الخليج العربية

العقيد الركن/ محمد أحمد آل حامد

17. الإمارات العربية المتحدة «آفاق وتحديات»

نخبة من الباحثين

18. أمن منطقة الخليج العربي من منظور وطني

صاحب السمو الملكي الفريق أول ركن
خالد بن سلطان بن عبدالعزيز آل سعود

19. السياسة الأمريكية في الشرق الأوسط والصراع العربي ـ الإسرائيلي

د. شبلي تلحمي

20. العلاقات الفلسطينية-العربية من المنفى إلى الحكم الذاتي

د. خليل شقاقي

21. أساسيات الأمن القومي: تطبيقات على دولة الإمارات العربية المتحدة

د. ديفيد جارنم

22. سياسات أسواق العمالة في دول مجلس التعاون لدول الخليج العربية

د. سليمان القدسي

23. الحركات الإسلامية في الدول العربية

خليل علي حيدر

24. النظام العالمي الجديد

ميخائيل جورباتشوف

25. العولمة والأقلمة: اتجاهان جديدان في السياسات العالمية

د. ريتشارد هيجوت

26. أمن دولة الإمارات العربية المتحدة: مقترحات للعقد القادم

د. ديفيد جارنم

27. العالم العربي وبحوث الفضاء: أين نحن منها؟

د. فاروق الباز

28. الأوضاع الاقتصادية والسياسية والأمنية في روسيا الاتحادية

د. فكتور ليبيديف

29. مستقبل مجلس التعاون لدول الخليج العربية

د. ابتسام سهيل الكتبي

د. جمال سند السويدي

اللواء الركن حيي جمعة الهاملي

سعادة السفير خليفة شاهين المرر

د. سعيد حارب المهيري

سعادة سيف بن هاشل المسكري

د. عبدالخالق عبدالله

سعادة عبدالله بشارة

د. فاطمة سعيد الشامسي

د. محمد العسومي

30. الإسلام والديمقراطية الغربية والثورة الصناعية الثالثة: صراع أم التقاء؟

د. علي الأمين المزروعي

31. منظمة التجارة العالمية والاقتصاد الدولي

د. لورنس كلاين

32. التعليم ووسائل الإعلام الحديثة وتأثيرهما في المؤسسات السياسية والدينية

د. ديل إيكلمان

33. خمس حروب في يوغسلافيا السابقة

اللورد ديفيد أوين

34. الإعلام العربي في بريطانيا

د. سعد بن طفلة العجمي

35. الانتخابات الأمريكية لعام 1998

د. بيتر جوبسر

36. قراءة حديثة في تاريخ دولة الإمارات العربية المتحدة

د. محمد مرسي عبدالله

37. أزمة جنوب شرقي آسيا: الأسباب والنتائج

د. ريتشارد روبيسون

38. البيئة الأمنية في آسيا الوسطى

د. فريدريك ستار

39. التنمية الصحية في دولة الإمارات العربية المتحدة من منظور عالمي

د. هانس روسلينج

40. الانعكاسات الاستراتيجية للأسلحة البيولوجية والكيماوية على أمن الخليج العربي

د. كمال علي بيوغلو

41. توقعات أسعار النفط خلال عام 2000 وما بعده ودور منظمة الأوبك

د. إبراهيم عبدالحميد إسماعيل

42. التجربة الأردنية في بناء البنية التحتية المعلوماتية

د. يوسف عبدالله نصير

43. واقع التركيبة السكانية ومستقبلها في دولة الإمارات العربية المتحدة

د. مطر أحمد عبدالله

44. مفهوم الأمن في ظل النظام العالمي الجديد

عدنان أمين شعبان

45. دراسات في النزاعات الدولية وإدارة الأزمة

د. ديفيد جارنم

46. العولمة: مشاهد وتساؤلات

د. نايف علي عبيد

47. الأسرة ومشكلة العنف عند الشباب (دراسة ميدانية لعينة من الشباب في جامعة الإمارات العربية المتحدة)

د. طلعت إبراهيم لطفي

48. النظام السياسي الإسرائيلي: الجذور والمؤسسات والتوجهات

د. بيتر جوبسر

49. التنشئة الاجتماعية في المجتمع العربي في ظروف اجتماعية متغيرة

د. سهير عبدالعزيز محمد

50. مصادر القانون الدولي: المنظور والتطبيق

د. كريستوف شرور

51. الثوابت والمتغيرات في الصراع العربي-الإسرائيلي وشكل الحرب المقبلة

اللواء طلعت أحمد مسلم

52. تطور نظم الاتصال في المجتمعات المعاصرة

د. راسم محمد الجمال

53. التغيرات الأسرية وانعكاساتها على الشباب الإماراتي:
تحليل سوسيولوجي

د. سعد عبدالله الكبيسي

54. واقع القدس ومستقبلها في ظل التطورات الإقليمية والدولية

د. جواد أحمد العناني

55. مشكلات الشباب: الدوافع والمتغيرات

د. محمود صادق سليمان

56. محددات وفرص التكامل الاقتصادي
بين دول مجلس التعـاون لدول الخليـج العربية

د. محمد عبدالرحمن العسومي

57. الرأي العام وأهميته في صنع القرار

د. بسيوني إبراهيم حمادة

58. جذور الانحياز: دراسة في تأثير الأصولية المسيحية
في السياسة الأمريكية تجاه القضية الفلسطينية

د. يوسف الحسن

59. ملامح الاستراتيجية القومية في النهج السياسي
لصاحب السمو الشيخ زايد بن سلطان آل نهيان
رئيس دولة الإمارات العربية المتحدة

د. أحمد جلال التدمري

60. غسل الأموال: قضية دولية

مايكل ماكدونالد

61. معضلة المياه في الشرق الأوسط

د. غازي إسماعيل ربابعة

62. دولة الإمارات العربية المتحدة: القوى الفاعلة في تكوين الدولة

د. جون ديوك أنتوني

63. السياسة الأمريكية تجاه العراق

د. جريجوري جوز الثالث

77. التطور التدريجي لمفاوضات البيئة الدولية:
من استوكهولم إلى ريودي جانيرو

مارك جيدوبت

78. اقتصـادات الخليـج العـربي: التحديات والفرص

د. إبراهيم عويس

79. الإسلام السياسي والتعددية السياسية من منظور إسلامي

د. محمد عمارة

80. إحصاءات الطاقة:
المنهجية والنماذج الخاصة بوكالة الطاقة الدولية

جون دينمان و ميكي ريسي و سوبيت كاربوز

81. عمليات قوات الأمم المتحدة لحفظ السلام:
تجربة أردنية

السفير عيد كامل الروضان

82. أنماط النظام والتغيرات في العلاقات الدولية:
الحـروب الكبرى وعواقبها

د. كيتشي فوجيوارا

83. موقف الإسلاميين من المشكلة السكانية وتحديد النسل

خليل علي حيدر

84. الدين والإثنية والتوجهات الأيديولوجية في العراق:
من الصراع إلى التكامل

د. فالح عبدالجبار

85. السياسة الأمريكية تجاه الإسلام السياسي

جراهام فولر

86. مكانة الدولة الضعيفة في منطقة غير مستقرة: حالة لبنان

د. وليد مبارك

87. العلاقات التجارية بين مجلس التعاون
لدول الخليج العربية والاتحاد الأوربي: التحديات والفرص

د. رودني ويلسون

88. احتمالات النهضة في "الوطن العربي" بين تقرير
التنمية الإنسانية العربية ومشروع الشرق الأوسط الكبير

د. نادر فرجاني

89. تداعيات حربي أفغانستان والعراق على منطقة الخليج العربي

د. أحمد شكارة

90. تشكيل النظام السياسي العراقي:
دور دول مجلس التعاون لدول الخليج العربية

جيمس راسل

91. الاستراتيجية اليابانية تجاه الشرق الأوسط
بعد أحداث الحادي عشر من سبتمبر

د. مسعود ضاهر

92. الاستخبارات الأمريكية بعد الحادي عشر من سبتمبر: سد الثغرات

إيلين ليبسون

93. الأمم المتحدة والولايات المتحدة والاتحاد الأوربي والعراق:
تحديات متعددة للقانون الدولي

ديفيد م. مالون

94. الحرب الأمريكية على الإرهاب وأثرها على العلاقات الأمريكية-العربية

جيمس نويز

95. القضية الفلسطينية وخطة الانفصال عن غزة:
آفاق التسوية.. انفراج حقيقي أم وهمي؟

د. أحمد الطيبي ومحمد بركة

96. حرب الولايات المتحدة الأمريكية على العراق
وانعكاساتها الاستراتيجية الإقليمية

د. أحمد شكارة

97. سيناريوهات المستقبل المحتملة في العراق

كينيث كاتزمان

98. الأسلحة النووية في جنوب آسيا

كريس سميث

110. أستراليا والشرق الأوسط: لماذا أستراليا "مؤيد صلب" لإسرائيل؟

علي القزق

111. العلاقات الأمريكية ـ الإيرانية: نظرة إلى الوراء... نظرة إلى الأمام

فلينت ليفيريت

112. نزاعات الحدود وحلها في ضوء القانون الدولي: حالة قطر والبحرين

جيوفاني ديستيفانو

113. العراق والإمبراطورية الأمريكية:
هل يستطيع الأمريكيون العرب التأثير في السياسة الأمريكية في الشرق الأوسط؟

د. رشيد الخالدي

114. الولايات المتحدة الأمريكية وأوربا في الشرق الأوسط وخارجه:
شركاء أم متنافسون؟

تشارلز كوبتشان

115. تعاظم دور حلف الناتو في الشرق الأوسط "الكبير"

فيليب جوردن

116. مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية

د. ناصر بن محمد البقمي

قسيمة اشتراك في سلسلة

«محاضرات الإمارات»

الاســـم : ....

المؤسسة : ....

العنـوان : ....

ص. ب : .... المـدينــــة : ....

الرمز البريدي : ....

الـــدولـة : ....

هـــاتـف : .... فـاكـــس : ....

البريد الإلكتروني : ....

بدء الاشتراك: (من العدد: .... إلى العدد : ....)

رسوم الاشتراك*

للأفـراد:	110 دراهم	30 دولاراً أمريكياً
للمؤسسات:	220 درهماً	60 دولاراً أمريكياً

- ❑ للاشتراك من داخل الدولة يقبل الدفع النقدي، والشيكات، والحوالات النقدية.
- ❑ للاشتراك من خارج الدولة تقبل فقط الحوالات المصرفية، مع تحمل المشترك تكاليف التحويل.
- ❑ في حالة الحوالـة المـصرفية، يرجـى تحويـل قيمـة الاشـتراك إلى حـساب مركـز الإمـارات للدراسـات والبحوث الاستراتيجية رقم 1950050565 ـ بنك أبوظبي الـوطني ـ فـرع الخالديـة، ص. ب: 46175 أبوظبي ـ دولة الإمارات العربية المتحدة.
- ❑ يمكن الاشتراك عبر موقعنا على الإنترنت (www.ecssr.ae) باستعمال بطاقتي الائتمان Visa وMaster Card.

لمزيد من المعلـومات حول آلية الاشتراك يرجى الاتصال:

قسم التوزيع والمعارض

ص.ب: 4567 أبوظبي ـ دولة الإمارات العربية المتحدة

هاتف: 4044445 (9712) فاكس: 4044443 (9712)

البريد الإلكتروني: books@ecssr.ae

الموقع على الإنترنت: http://www.ecssr.ae

* تشمل رسوم الاشتراك الرسوم البريدية، وتغطي تكلفة اثني عشر عدداً من تاريخ بدء الاشتراك.